

明 細 書

ポリシールール適用ネットワークシステム

技術分野

本発明は、ポリシールール適用ネットワークシステムに関し、特にシングルポリシールールが運用に伴って単調に増大することを抑制可能にしたり、ネットワーク運用者の負担を格段に減少させることを可能にするポリシールール適用ネットワークシステムに関する。

背景技術

近年、インターネットへのアクセス方式として、ADSL (Asymmetric Digital Subscriber Line) 及びFTTH (Fiber to the Home) 等のブロードバンド・アクセス方式が一般的となってきた。キャリア（通信キャリアまたは通信事業者）、ISP (Internet Service Provider)、及びIDC (Internet Data Center) 等のサービス提供者が、このブロードバンド・アクセス方式のサービス提供を開始している。その結果、ネットワーク内を流れるトラフィックが飛躍的に増加している。

この様なトラフィックの増加に伴い、ネットワークを構成するネットワーク機器に対する処理負荷が高くなり、ネットワーク内でのパケットの転送遅延や破棄が発生し、サービス品質 (QoS : Quality of Service) を劣化させる要因となっている。そのため、広帯域情報サービスや双方向音声通信サービス等を提供する上記サービス提供者は、サービス利用者（ユーザ）に対して、安定したサービス品質を提供するためのネットワーク運用手順を講ずる事が要求されている。これにより、ネットワーク運用者（管理者）は、ネットワーク運用状況に応じた最適なポリシールールを生成する必要があるが、運用状況により多数のポリシールールを生成する事になり、ネットワーク運用者への負担が増加している。

さらに、ネットワークを構成する各ネットワーク機器に対して、複数のポリシールールを適用したいというネットワーク運用者からの要望がある。例えば、「特定の経路のトラフィックが輻輳したら、トラフィックの経路を変更すると共に、ネットワークに流れ込むトラフィックもある割合で抑制したい」とか、「特定の経路の回線が障害とな

ったら、トラヒックの経路を変更すると共に、ネットワーク運用者への通知を行う」等がある。このようなネットワーク運用者からの要望に対して、柔軟に対応できるポリシールール適用手法（方法、技術）が必要となっている。

ここで、MPLS (Multi Protocol Label Switching) ネットワーク等の IP (Internet Protocol) ネットワークをポリシーサーバにより運用する従来の一手法について説明する。

ポリシーサーバは、ネットワーク運用者がネットワークの運用状況に応じて、各種ネットワーク運用ポリシーを設定すると、この設定されたポリシーをネットワーク内に存在する個々のネットワーク機器の動作設定のために自動的に反映させるものである。

ネットワーク運用者が設定する各種運用ポリシーは、条件（コンディション）とそれに対応する動作（アクション）により構成されるポリシールールである。従来のポリシーサーバにおいては、送信元の IP アドレス、サブネットマスク及びポート番号等と、送信先（宛先）の IP アドレス、サブネットマスク及びポート番号等とのパケットのヘッダ情報を条件として用いるか、ポリシーを適用する時間帯を条件とすることが一般的である。

これらのポリシー情報は、ネットワーク運用者が予め決定するネットワークの運用指針に従って作成される。

しかし、上述した従来の一手法を用いても、次のような問題が残存する。現在、運用されているようなプリミティブなポリシーでは、運用が進むにつれて、ネットワーク運用者が管理・運用するポリシーが単調増加してしまい、効果的な運用を阻害してしまう。

また、ポリシールールをマクロ的な観点で把握するような管理・運用手法になっていないため、運用コストが増大すると共に、ポリシールールの階層的な管理が行えていない。

さらに、運用ポリシーは、ネットワークの運用状況に応じて、数多く作成されたポリシーの中から、ネットワーク運用者が最適なポリシーを決定し、運用するネットワークに対して適用するが、数多くのポリシーを作成した場合、管理が難しくなり、最適なポリシーを選定する事も困難となる。

また、同一出願人による先願である特願 2003-22731（2003 年 1 月 30 日出願）において提案されているように、ネットワーク運用状況に基づいて、適用するポリシーを追加したり、適用されているポリシーを変更したり、適用されているポリシーの差し替えを行うネットワーク運用状況に基づくポリシー適用手法がある。

しかし、このポリシー適用手法を採用した場合においても、適用されるポリシーは単独で存在する極めてプリミティブなシングルポリシーである。シングルポリシーだけに基づいて、適用するポリシーを追加したり、適用されているポリシーの変更や差し替えを行うと、システム負荷を増大すると共に、上述したようにネットワーク運用者の運用負荷を更に増長することを免れない。

〔特許文献 1〕

特開 2002-204254 号公報

発明の開示

本発明の課題は、シングルポリシールールが運用に伴って単調に増大することを抑制可能な手法を提供することにある。

本発明の他の課題は、ネットワーク運用者の負担を格段に減少させることが可能な手法を提供することにある。

上記課題を解決するために、本発明の第 1 のポリシー制御装置は、管理対象ネットワークの運用状況（状態）の変遷に応じて、前記ネットワーク内に存在する個々のネットワーク機器の動作設定のために、コンディションとこれに対応するアクションとにより規定されるポリシールールを反映させるポリシー制御装置であって；

同一コンディションで異なるアクションのシングルポリシールールの少なくとも 2 つを組み合わせ単位として生成された複数のマルチポリシールールを適用対象ネットワーク機器の特定情報とともに更新可能に格納する記憶手段と；

この記憶手段に格納されている前記複数のマルチポリシールールのいずれかを前記特定情報に基づいて識別した前記ネットワーク機器の動作設定のために適用する制御手段とを備える。

本発明の第 2 のポリシー制御装置は、管理対象ネットワークの運用状況の変遷に応じて、前記ネットワーク内に存在する個々のネットワーク機器の動作設定のために、

コンディションとこれに対応するアクションとにより規定されるポリシールールを反映させるポリシー制御装置であって；

同一コンディションで異なるアクションの複数のシングルポリシールールを適用対象ネットワーク機器の特定情報及び適用優先度情報とともに更新可能に格納する記憶手段と；

前記優先度情報に基づく優先順位で、前記記憶手段に格納されている前記複数のシングルポリシールールのいずれかを前記特定情報に基づいて識別した前記ネットワーク機器の動作設定のために適用する制御手段とを備える。

本発明の第 1 または第 2 のポリシー制御装置において、前記コンディションは、前記管理対象ネットワークの運用状況を示す、回線障害、トラヒック量閾値超過、及びパケットロス量閾値超過の少なくとも 1 つを含み、前記アクションは、トラヒックの流れる経路の切替、トラヒックを抑制するためのフロー制御、及びネットワーク運用者への通知の少なくとも 2 つを含む。

また、前記適用対象ネットワーク機器の特定情報は、前記ネットワーク機器の識別情報及び回線インタフェースの識別情報を含む。

また、前記複数のマルチポリシールールのそれぞれは、前記ポリシールールの階層的管理を可能にするために、前記記憶手段に予め登録された同一コンディションで異なるアクションの前記シングルポリシールールの少なくとも 2 つを組み合わせ単位として生成される。

また、前記記憶手段は、更に前記複数のマルチポリシールールの適用優先度情報を更新可能に格納し、前記制御手段は、前記優先度情報に基づく優先順位で前記複数のマルチポリシールールのいずれかを前記ネットワーク機器の動作設定のために適用する。

さらに、前記記憶手段は、更に前記複数のマルチポリシールールのそれぞれ内の前記シングルポリシールールの適用優先度情報を更新可能に格納し、前記制御手段は、前記優先度情報に基づく優先順位で前記複数のマルチポリシールールのそれぞれ内の前記シングルポリシールールを前記ネットワーク機器の動作設定のために適用する。

本発明の第 1 のポリシー制御方法は、管理対象ネットワークの運用状況の変遷に応じて、前記ネットワーク内に存在する個々のネットワーク機器の動作設定のために、

コンディションとこれに対応するアクションとにより規定されるポリシールールを反映させるポリシー制御方法であって；

同一コンディションで異なるアクションのシングルポリシールールの少なくとも2つを組み合わせ単位として生成された複数のマルチポリシールールを適用対象ネットワーク機器の特定情報とともに更新可能に格納し；

格納されている前記複数のマルチポリシールールのいずれかを前記特定情報に基づいて識別した前記ネットワーク機器の動作設定のために適用する。

本発明の第2のポリシー制御方法は、管理対象ネットワークの運用状況の変遷に応じて、前記ネットワーク内に存在する個々のネットワーク機器の動作設定のために、コンディションとこれに対応するアクションとにより規定されるポリシールールを反映させるポリシー制御方法であって；

同一コンディションで異なるアクションの複数のシングルポリシールールを適用対象ネットワーク機器の特定情報及び適用優先度情報とともに更新可能に格納し；

前記優先度情報に基づく優先順位で、格納されている前記複数のシングルポリシールールのいずれかを前記特定情報に基づいて識別した前記ネットワーク機器の動作設定のために適用する。

本発明によれば、シングルポリシールールを組み合わせたマルチポリシールールを適用可能にすることにより、シングルポリシールールが運用と共に単調に増大することを抑制できる。

また、本発明によれば、運用する上でも、シングルポリシールールを選択するだけで、マクロ的な観点で把握し管理できるマルチポリシールールを作成する事ができるので、ネットワーク運用者の負担を格段に減少させる事ができる。

さらに、本発明によれば、ポリシールール（シングルポリシールール及びマルチポリシールール）に対して優先順位（優先度）を設定することにより、同時に複数のポリシールールを設定する事ができ、かつネットワーク運用状況に応じて、複数のポリシールールの中から優先順位に従った最適なポリシールールが自動的に選択される事により、ネットワーク運用者の管理負担が格段に減少する。加えて、ネットワークシステム自体の動作の効率化も図ることができる。

本発明の他の課題、特徴及び利点は、図面及び併記の特許請求の範囲とともに取り

上げられる際に、以下に記載される明細書（実施形態）を読むことにより明らかになるであろう。

図面の簡単な説明

図 1 は本発明の一実施の形態のシステム及びポリシーサーバの構成を示すブロック図；

図 2 は本発明の一実施の形態のシステムにおいて適用されるポリシールールを説明するための図；

図 3 はポリシールールの登録シーケンスを示す図；

図 4 は優先度付けポリシールールの登録シーケンスを示す図；

図 5 はポリシールール適用の処理シーケンスを示す図；

図 6 はポリシーサーバのユーザインタフェース手段の処理フローを示す図；

図 7 はポリシーサーバのポリシー管理手段の処理フローを示す図；

図 8 はポリシーサーバのポリシー分析手段の処理フローを示す図；

図 9 はポリシーサーバのネットワーク運用情報収集手段の処理フローを示す図；

図 10 はポリシーサーバのネットワーク監視手段の処理フローを示す図；

図 11 はポリシーサーバのネットワーク状況分析手段の処理フローを示す図；

図 12 はポリシーサーバの最適ポリシー選択手段の処理フローを示す図；

図 13 はポリシーサーバのポリシー適用指示手段の処理フローを示す図；

図 14 はポリシーサーバのポリシー適用手段の処理フローを示す図；

図 15 はポリシーサーバの関連処理実行手段の処理フローを示す図；

図 16 はポリシーサーバのポリシー管理データベースにて管理する情報のデータ構造を示す図；

図 17 はポリシーサーバのポリシー分析データベースにて管理する情報のデータ構造を示す図；及び

図 18 はポリシーサーバのネットワーク管理データベースにて管理する情報のデータ構造を示す図である。

発明を実施するための最良の形態

以下、添付図面を参照して、本発明についてさらに詳細に説明する。図面には本発明の好ましい実施形態が示されている。しかし、本発明は、多くの異なる形態で実施されることが可能であり、本明細書に記載される実施形態に限定されると解釈されてはならない。むしろ、これらの実施形態は、本明細書の開示が徹底的かつ完全となり、当業者に本発明の範囲を十分に伝えるように提供される。明細書及び図面の全体を通じて同一参照番号は同一の構成要素を指す。

〔システムの構成〕

本発明の一実施の形態におけるシステム構成を示す図1を参照すると、ポリシールール適用ネットワークシステム1はポリシーサーバ（ポリシー制御装置）2及びIP（Internet Protocol）ネットワーク3から構成されている。

IPネットワーク3は、具体的には、MPLS（Multi Protocol Label Switching）ネットワークなどのラベルスイッチネットワークであり、IPパケットの転送処理にラベルという新しい概念を導入し、IPレベル（レイヤ3）でのルーティング処理をATM（Asynchronous Transfer Mode）、フレームリレー、及びEthernetなどの下位レイヤ（レイヤ2）のスイッチング処理で実現するMPLS技術を採用している。IPネットワーク（特に、限定を要しないときは、単にネットワークと記載する）3は、ネットワーク機器としての複数のノード4、5、6、7を備えている。

ポリシーサーバ2はIPネットワーク3の入口に配置されたノード4と物理的な回線（物理リンク）によって接続されている。このネットワーク3の入口に配置されたノード4とネットワーク3の出口に配置されたノード7とは、中継（コア）ノード5、6及び物理的な回線（物理リンク）を通して接続されている。入口ノード4及び出口ノード7は、他のIPネットワーク（図示省略）にそれぞれ接続される。

この構成を採るポリシールール適用ネットワークシステム1においては、後に詳述するように、ポリシーサーバ2はユーザ情報及びポリシー（運用指針）情報とネットワーク全体の状態（運用状況）とに基づき、ノード4～7の動作を決定する。ポリシーサーバ2はIPフロー毎の最適経路設定（QoSを考慮した明示的な経路（ルート）設定、IPフローのアグリゲート（集約））及びトラヒックの負荷分散などのトラフィックエンジニアリングに関するサービスを提供するために、COPS（Common Open Policy Service）などのポリシー制御プロトコルに則って、ノード4～7を集中的に

制御する。

また、入口ノード4、中継ノード5、6、及び出口ノード7は、IPパケットを送送（転送及び交換などを含む）するルータ及びスイッチなどのネットワーク機器によって構成され、ポリシーサーバ2の決定に従った動作を実行する。入口ノード4はポリシーサーバ2とポリシー制御プロトコルに則って直接に情報を送受信するが、中継ノード5、6及び出口ノード7は入口ノード4を通してポリシーサーバ2と情報の送受信を行う。

〔システムの機能〕

図1に示すポリシールール適用ネットワークシステム1においては、ネットワーク運用者（管理者）が保守・運用端末を利用し、ポリシーサーバ2のユーザインタフェース手段101を介して作成したプリミティブなポリシーであるシングルポリシールール、もしくはポリシーサーバ2において予め提供されたテンプレートをカスタマイズして作成したシングルポリシールールを組み合わせることで、複数のシングルポリシールールで構成されたマルチポリシールールを作成することを許容する機能を有する。これにより、マクロな観点で捉えたポリシールール適用を可能とし、ネットワーク運用者の運用管理負荷を抑制することを可能とする。

また、ネットワーク運用者がシングルポリシールール自体に優先度を設定したり、マルチポリシールールを構成するシングルポリシールール毎に優先度を設定するなどにより、ネットワークに適用すべき最適ポリシーを系統的に効率良く、かつネットワーク運用者の意図を十分に反映した形で、ポリシールールに応じたネットワーク運用を可能とする機能を有する。

ここで、図2（A）、（B）を参照して、シングルポリシールールとマルチポリシールールとについて説明する。

図2（A）は、トラヒックエンジニアリングに関連するネットワークに対するシングルポリシールールを示している。図2（B）は、ネットワーク運用者がシングルポリシーを自由に組み合わせて作成可能なマルチポリシールールを示している。

このポリシールール適用ネットワークシステム1においては、図2（B）に示すように、ネットワーク運用者が、図2（A）に示すシングルポリシールールを複数組み合わせ合わせたマルチポリシールールを作成し、随時変遷するネットワーク運用状況に応じ

たポリシールールをきめ細かく、かつ判り易く生成することを可能にしている。

例えば、ネットワーク運用者は、図2 (A) におけるポリシールール1「回線(回線単位) 障害発生時に経路切替を実施するポリシー」と、ポリシールール3「回線障害発生時にネットワーク運用者へメール通知するポリシー」との同一コンディションで異なるアクションの2つのシングルポリシールールを組み合わせることにより、

「回線障害発生時に経路切替を実施し、かつ実施したことをネットワーク運用者にメールで通知する」といった、図2 (B) に示す新たなポリシールール(マルチポリシールール) 11を容易に作成することが可能となる。

また、ネットワーク運用者は、図2 (A) におけるポリシールール1「回線障害発生時に経路切替を実施するポリシー」と、ポリシールール2「回線障害発生時にフロー制御を実施するポリシー」と、ポリシールール3「回線障害発生時にネットワーク管理者へメール通知するポリシー」との同一コンディションで異なるアクションの3つのシングルポリシールールを組み合わせることにより、「回線障害発生時に経路切替を実施し、その切り替えた経路へは特定のフローを規制し、かつこれらのポリシーが実施されたことをネットワーク運用者にメール通知する」といった、一層木目細かい新たなポリシールール(マルチポリシールール) 13を容易にかつ判りやすく作成することも可能とする。

次に、図2 (A), (C) を参照して、優先度を考慮した場合について説明する。図2 (C) は、マルチポリシールールを構成するシングルポリシーに対してネットワーク運用者が自由に設定可能である優先度(プライオリティ) を割付けた優先度付きポリシールールを示している。

図2 (C) に示すように、図2 (A) における各ポリシールール1~9に論理的パス(例えば、MPLSネットワークにおけるラベルスイッチパス) 毎の優先度を付与し、マルチポリシールールが適用される際にその優先度に応じて、シングルポリシールールを選択し実行することにより、ネットワーク運用者が、随時変遷するネットワーク運用状況に応じたシングルポリシールールを木目細かくかつ柔軟に生成することが可能となる。

例えば、図2 (C) におけるパス名「Tunnel-1」には、マルチポリシールール10を構成する同一コンディションの2つのシングルポリシールール1, 2が割

り当てられており、ポリシールール1は、ポリシールール2よりも実行優先度が高いため、マルチポリシールール10を適用することは、必ずポリシールール1が優先的に選択され実行される。また、ネットワーク運用者は、図2（C）における各シングルポリシールールの実行優先度をネットワーク運用状況に応じて容易に変更することも可能である。

なお、このポリシールール適用ネットワークシステム1においては、ネットワーク運用者がシングルポリシールール間の優先度付け（図2（A）参照）及びマルチポリシールール間の優先度付け（図2（B）参照）を同一コンディションのポリシールールを単位として設定することも可能である。

ネットワーク運用者がポリシーサーバ2のユーザインタフェース手段101を介して作成した上述の各ポリシールールは、後に詳述するように、マルチポリシー管理手段102を通してポリシー管理データベース110に登録（格納）されることになる。上記図2（C）におけるパス名は、後に詳述するポリシー管理データベース110内の条件（コンディション）とリンクージする。

〔ポリシーサーバの構成・機能〕

図1を参照すると、ポリシーサーバ2は、管理対象ネットワークの運用状況の変遷に応じて、ネットワーク3内に存在する個々のノード（ネットワーク機器）の動作設定のために、条件（コンディション）とこれに対応する動作（アクション）とにより規定されるポリシールールを反映させる。

このために、ポリシーサーバ2は、同一コンディションで異なるアクションのシングルポリシールールの少なくとも2つを組み合わせ単位として生成された複数のマルチポリシールールを適用対象ネットワーク機器の特定情報とともに更新可能に格納し、格納されている複数のマルチポリシールールのいずれかを上記特定情報に基づいて識別したネットワーク機器の動作設定のために適用する。

また、ポリシー制御装置2は、同一コンディションで異なるアクションの複数のシングルポリシールールを適用対象ネットワーク機器の特定情報及び適用優先度情報とともに更新可能に格納し、優先度情報に基づく優先順位で、格納されている複数のシングルポリシールールのいずれかを上記特定情報に基づいて識別したネットワーク機器の動作設定のために適用する。

詳述すると、ポリシーサーバ2におけるユーザインタフェース手段(部)101は、ネットワーク運用者が保守・運用端末(図示省略)を通してシングルポリシールールの作成、シングルポリシールールへの優先順位付け、シングルポリシールールを組み合わせたマルチポリシールールの作成、マルチポリシールールへの優先順位付け、マルチポリシールール内のシングルポリシールールへの優先順位付け、及び各ポリシー情報の登録要求を行うためのユーザインタフェース(GUI: Graphical User Interface)を提供する。

ポリシー管理手段102は、ネットワーク運用者がユーザインタフェース手段101を介して作成したポリシールール(シングルポリシールール、マルチポリシールール)をポリシー管理データベース(DB)110に格納して管理する。

ポリシー分析手段201は、ポリシー管理手段102を介してポリシー管理データベース110に登録されたポリシールールを分析し、各種ポリシールールとネットワーク運用状況との関連付けを行い、ポリシー分析データベース210を用いて管理する。

ネットワーク運用情報収集手段301は、ポリシー分析手段201からの要求を受け、ネットワーク運用状況の収集対象となるネットワーク機器のネットワーク機器情報についてネットワーク管理データベース310を用いて管理する。

ネットワーク監視手段302は、IPネットワーク3から収集した情報をネットワーク管理データベース310にて管理すると共に、定期的にネットワーク管理データベース310を参照し、ネットワーク運用状況に変化があるか否かを監視する。

ネットワーク監視手段302は、監視対象の情報をネットワーク管理データベース310から読出し、各対象ネットワーク機器からネットワーク監視状況情報を収集する。

上記ネットワーク運用情報収集手段301は、ネットワーク運用状況に変化があった場合は、ネットワーク監視手段302によって収集された情報をネットワーク管理データベース310より読出し、ネットワーク状況分析手段303へ通知する。

ネットワーク状況分析手段303は、通知されたネットワーク運用状況を分析し、最適ポリシー選択手段304へ通知する。最適ポリシー選択手段304は、通知されたネットワーク運用状況情報より、優先順位等を用いた最適なポリシールールの選択

を行い、ポリシー適用指示手段 305 へ通知する。

ポリシー適用指示手段 305 は、通知されたポリシールールを分析し、ポリシールール内の動作（アクション）の内容や優先順位に従い、ポリシー適用手段 306 及び関連処理実行手段 307 に処理を要求する。処理要求後、ポリシー分析 DB 210 の該当ポリシールールの適用状態を適用に設定する。

ポリシー適用手段 306 は、適用対象のネットワーク機器に対して、ポリシールールに応じたネットワーク制御を行う。また、関連処理実行手段 307 はネットワーク機器に対するネットワーク制御以外のメール通知等の関連処理を行う。

〔動作概要〕

次に、図 1 に示す本発明の一実施の形態のシステムにおける動作の概要を説明する。

図 3 はポリシールールの登録を行う際のシーケンスを示す。図 4 は優先度付けのポリシールールの登録を行う際のシーケンスを示す。図 5 はポリシールール適用を行う際のシーケンスを示す。

まず、図 1 及び図 3 を併せ参照して、シングルポリシールール及びマルチポリシールールの登録を行う際の動作について説明する。

ネットワーク運用者は、ポリシーサーバ 2 に IP ネットワーク 3 を経由して接続されている保守・端末装置を利用して（なお、特に限定を要しないときは、この端末の介在を省略する）、シングルポリシールールの作成をユーザインタフェース手段 101 を介して行う。このためには、ネットワーク運用者はシングルポリシールールを予め作成する必要がある。そして、ネットワーク運用者は登録した複数のシングルポリシールールを組み合わせ、マクロ的な観点でポリシールールを管理し、かつ木目細かいポリシールールの作成を可能とするマルチポリシールールの作成をユーザインタフェース手段 101 を介して行う。さらに、ネットワーク運用者は適用可能となるノード（ネットワーク機器）へのマルチポリシールールの関連付け登録を行う。

ネットワーク運用者からのこの登録操作においては、ユーザインタフェース手段 101 からポリシー管理手段 102 に対して、シングルポリシールール登録（シーケンス SS01）、マルチポリシールール登録（シーケンス SS02）、及び適用対象ノード指定に伴うマルチポリシールール設定に関する各種要求が行われ、ポリシー管理手段 102 はシングルポリシールール及びマルチポリシールールのポリシー情報を関

連付け情報と共にポリシー管理データベース 110 に登録（格納、更新）する。

そして、ポリシー管理手段 102 は、ポリシー分析手段 201 に対して、ポリシールールが登録された旨の通知を行う。ポリシー分析手段 201 は、通知された情報を分析し、ポリシー情報をポリシー分析データベース 210 に格納すると共に、ネットワーク運用状況変化を監視するポイントをネットワーク運用情報収集手段 301 に対して通知する。これにより、ネットワーク運用情報収集手段 301 はネットワーク運用状況変化を監視するポイント、つまり情報収集対象のネットワーク機器に対応する情報をネットワーク管理データベース 310 に格納する。

次に、図 1 及び図 4 を併せ参照して、優先度付けのシングルポリシールールまたは優先度付けのマルチポリシールールの登録を行う際の動作について説明する。

ネットワーク運用者は、ポリシーサーバ 2 に接続されている保守・端末装置を利用して、シングルポリシールールの作成をユーザインタフェース手段 101 を介して行う。このためには、ネットワーク運用者はシングルポリシールールを予め作成する必要がある。そして、ネットワーク運用者は登録した複数のシングルポリシールールを組み合わせ、マクロ的な観点でポリシールールを管理し、かつ木目細かいポリシールールの作成を可能とするマルチポリシールールの作成を優先度付きでユーザインタフェース手段 101 を介して行う。さらに、ネットワーク運用者は適用可能となるノード（ネットワーク機器）へのマルチポリシールールの関連付け登録を行う。

ネットワーク運用者からのこの登録操作においては、ユーザインタフェース手段 101 からポリシー管理手段 102 に対して、シングルポリシールール登録（図 3 中のシーケンス S S 01）、マルチポリシールール登録（図 3 中のシーケンス S S 02）、及び適用対象ノード指定に伴うマルチポリシールール設定に関する各種要求が行われ、ポリシー管理手段 102 はシングルポリシールール及びマルチポリシールールのポリシー情報を関連付け情報やネットワーク運用者が指定を行った優先度情報と共にポリシー管理データベース 110 に登録（格納、更新）する。

そして、ポリシー管理手段 102 は、ポリシー分析手段 201 に対して、ポリシールールが登録された旨の通知を行う。ポリシー分析手段 201 は、通知された情報を分析し、ポリシー情報をポリシー分析データベース 210 に格納すると共に、ネットワーク運用状況変化を監視するポイントをネットワーク運用情報収集手段 301 に対

して通知する。これにより、ネットワーク運用情報収集手段 301 はネットワーク運用状況変化を監視するポイント、つまり情報収集対象のネットワーク機器に対応する情報をネットワーク管理データベース 310 に格納する。

なお、優先度付けのシングルポリシールール登録を行う際には、図 3 及び図 4 に示す登録シーケンスにおいて、ネットワーク運用者が、ユーザインタフェース手段 101 からポリシー管理手段 102 に対して、優先度付けシングルポリシールール登録と、適用対象ノード指定に伴うシングルポリシールール設定とに関する各種要求を行うことにより、同様に実施できる。

次に、図 1 及び図 5 を併せ参照して、シングルポリシールールまたはマルチポリシールール適用を行う際の動作について説明する。

ネットワーク運用情報収集手段 301 は、ネットワーク管理データベース 310 を参照して、定期的にネットワーク運用状況に変化があるか否かの判定を行っており、ネットワーク運用状況に変化があった場合は、収集情報の通知をネットワーク情報分析手段 303 に対して行う。

ネットワーク状況分析手段 303 は、通知された収集情報がシングルポリシールールまたはマルチポリシールールを適用する必要があるネットワーク運用状況変化が発生しているか否かの判定を行い、シングルポリシールールまたはマルチポリシールールの適用が必要な場合は、ポリシー適用要求を最適ポリシー選択手段 304 に対して通知する。

通知を受けた最適ポリシー選択手段 304 は、ポリシー分析データベース 210 を参照し、ネットワーク運用状況変化に伴う適用が可能であるシングルポリシールールまたはマルチポリシールールの一覧を作成し、その中から適用するポリシールールをシステムが持つ優先度（例えば、シングルポリシー登録順やシングルポリシーが属性として持つ優先度等）やネットワーク運用者が設定した優先度を参照して、ポリシールールの抽出を行う。また、最適ポリシー選択手段 304 は、抽出したポリシールール一覧から最適ポリシールールを決定する。

決定した最適ポリシールールは最適ポリシー選択手段 304 からポリシー適用指示手段 305 に対して通知され、ポリシー適用指示手段 305 は、ノード（ネットワーク機器）に対するネットワーク制御か、メール通知等のネットワーク制御以外の関連

処理かを判定し、ノードに対するネットワーク制御の場合は、ポリシー適用手段 306 に対してネットワーク制御指示（ポリシー適用指示）を行い、ネットワーク制御以外の場合は、関連付けられた処理対応のメール通知を実行する指示を関連処理実行手段 307 に対して行うことで、複数のアクションを実行することを可能とする。

〔具体的動作例〕

次に、図 1 に示す本発明の一実施の形態のシステムにおける具体的な動作例について、図 1 から図 18 を併せ参照して説明する。

〈前提条件〉

上述したように、図 1 に示すポリシールール適用ネットワークシステム 1 における IP ネットワーク 3 は、ネットワーク機器としての複数のノード 4, 5, 6, 7 を備えている。以下の動作では、複数のノード 4, 5, 6, 7 がネットワーク機器 A, B, C, D にそれぞれ対応するとして説明する。

ここでは、ネットワーク機器 A, B, C, D は、代表アドレス（各ネットワーク機器を特定するための IP アドレス）として、172.27.1.1、172.27.2.1、172.27.3.1、172.27.4.1 をそれぞれ持つ（割り当てられている）ものとする。

ネットワーク機器 A は、ネットワーク機器 A が持つ IP アドレス 172.27.1.0.1 のインタフェースでネットワーク機器 B に接続し、ネットワーク機器 A が持つ IP アドレス 172.27.50.1 のインタフェースでネットワーク機器 C に接続し、かつネットワーク機器 A が持つ IP アドレス 172.27.60.1 のインタフェースでネットワーク機器 D に接続するために、物理的な回線（物理リンク）上のパスを割り当てられる。

同様に、ネットワーク機器 B は、ネットワーク機器 B が持つ IP アドレス 172.27.10.2 のインタフェースでネットワーク機器 A に接続し、ネットワーク機器 B が持つ IP アドレス 172.27.20.1 のインタフェースでネットワーク機器 C に接続し、かつネットワーク機器 B が持つ IP アドレス 172.27.40.1 のインタフェースでネットワーク機器 D に接続するために、物理リンク上のパスを割り当てられる。

ネットワーク機器 C は、ネットワーク機器 C が持つ IP アドレス 172.27.5

0. 2のインタフェースでネットワーク機器Aに接続し、ネットワーク機器Cが持つIPアドレス172. 27. 20. 2のインタフェースでネットワーク機器Bに接続し、かつネットワーク機器Cが持つIPアドレス172. 27. 30. 1のインタフェースでネットワーク機器Dに接続するために、物理リンク上のパスを割り当てられる。

さらに、ネットワーク機器Dは、ネットワーク機器Dが持つIPアドレス172. 27. 60. 2のインタフェースでネットワーク機器Aに接続し、ネットワーク機器Dが持つIPアドレス172. 27. 40. 2のインタフェースでネットワーク機器Bに接続し、かつネットワーク機器Dが持つIPアドレス172. 27. 30. 2のインタフェースでネットワーク機器Cに接続するために、物理リンク上のパスを割り当てられる。

ここでは、更に次のような前提を置く。ネットワーク機器Aには、IPアドレス172. 27. 100. 1のサービス利用者（ユーザ）の使用する端末（ユーザ端末）Xが接続され、かつネットワーク機器Cには、IPアドレス172. 27. 200. 1のユーザ端末Yが接続されている。

ポリシーサーバ2は、IPアドレスとして172. 27. 150. 1を持ち、かつメールアドレスとしてp s e r v e r @ x y z . c o mを設定されている。

ネットワーク機器Aからネットワーク機器Cに直接流れるトラヒック（IPフロー）の経路を「ルート1」とし、かつネットワーク機器A、ネットワーク機器B及びネットワーク機器Cと流れるトラヒックの経路を「ルート2」とする。

また、ネットワーク運用者が作成するポリシールールは、条件（コンディション）と動作（アクション）とから構成される。この条件としては、対象物であるIPネットワーク3を流れるトラヒックがどのような状態（つまり、トラヒックの流れる回線が障害、トラヒック量閾値超過、パケットロス量閾値超過等）になった場合等の条件を指定できるものとする。動作としては、条件に対してどのような動作（トラヒックの流れる経路の切替、トラヒックを抑制するためのフロー制御、ネットワーク運用者へ通知するためのメール通知等）をするかを指定できるものとする。

〈第1の動作例〉

第1の動作例のポリシールール適用ネットワークシステム1においては、同一コン

ディションのシングルポリシールールを運用用途に応じて組み合わせてマルチポリシールールを作成することにより、多様化し瞬時に状況が変遷していくIPネットワーク3を柔軟に制御することを可能にしている。

図3に示すように、ネットワーク運用者は、ポリシーサーバ2にIPネットワーク3を経由して接続される保守・運用端末を利用して、条件（コンディション）として、ユーザ端末Xからユーザ端末Yへルート1で流れるトラヒック（IPフロー）に対して回線単位の障害発生時「条件1」、動作（アクション）として、ユーザ端末Xからユーザ端末Yへルート2でトラヒックが流れる様に経路切替「動作1」を行う「ポリシールール1」を指定し、ユーザインタフェース手段101を介してポリシールールの登録要求を行う（図6中のS10101、S10102）。

同様に、ネットワーク運用者は、コンディションとして、ユーザ端末Xからユーザ端末Yへルート1で流れるトラヒックに対して回線単位の障害発生時「条件2」、アクションとして、ネットワーク運用者へメール通知「動作2」を行う「ポリシールール3」を指定し、ユーザインタフェース手段101を介してポリシールールの登録要求を行う（図6中のS10101、S10102）。

これらのポリシールールの登録要求を受けたポリシー管理手段102は、ポリシー管理データベース110のポリシールール管理データ構造（図16参照）に基づき、「ポリシールール1」の場合は、ポリシー名に「ポリシールール1」、ポリシー種別に「シングルポリシー」、コンディションに「条件1」、アクションに「動作1」となるインスタンス110-P1を生成し、かつ「ポリシールール3」の場合、ポリシー名に「ポリシールール3」、ポリシー種別に「シングルポリシー」、コンディションに「条件2」、アクションに「動作2」となるインスタンス110-P2を生成し、ポリシールールとしてポリシー管理データベース110へ格納する（図7中のS10201～S10203）。

なお、「ポリシールール1」及び「ポリシールール3」は、それぞれコンディションとアクションとが1対1となるシングルポリシールールであるため、これらのポリシールールをネットワーク機器自体へ登録する事も可能である。

次に、ネットワーク運用者は、「ポリシールール1」及び「ポリシールール3」を指定し、これらのシングルポリシールールを組み合わせた「ポリシールール11」を

マルチポリシールールとして作成し、このマルチポリシールールの適用対象のネットワーク機器を指定することにより、ユーザインタフェース手段101を介してマルチポリシールールの登録要求が行える（図6中のS10101, S10102）。ここでは、「ポリシールール11」の適用対象のネットワーク機器がノード4に対応するネットワーク機器Aであるので、ネットワーク運用者はネットワーク機器ID「172.27.1.1」及びインタフェースID（回線インタフェースID）「172.27.50.1」を指定する。

このマルチポリシールールの登録要求を受けたポリシー管理手段102は、ポリシー管理データベース110のポリシールール管理データ構造（図16参照）に基づき、ポリシールール名に「ポリシールール11」、ポリシー種別に「マルチポリシー」、コンディションに「ブランク」、アクションに「ブランク」となるインスタンス110-P3を生成し、ポリシールールとしてポリシー管理データベース110へ格納する（図7中のS10201, S10204, S10205）。

また、ポリシー管理手段102は、マルチポリシールールとしての「ポリシールール11」を構成する2つのシングルポリシールール「ポリシールール1」及び「ポリシールール3」を「ポリシールール11」の配下に設定するために、ポリシー管理データベース110のマルチポリシールール配下管理データ構造（図16参照）に基づき、格納済の「ポリシールール1」及び「ポリシールール3」のポリシー情報を参照して、ポリシー名、ポリシー種別、コンディション、アクションからそれぞれ構成されるインスタンス110-P3-1及びインスタンス110-P3-2を生成する。そして、ポリシー管理手段102は、インスタンス110-P3の次ポインタ（Next Policy）にインスタンス110-P3-1を設定し、かつインスタンス110-P3-1の次ポインタにインスタンス110-P3-2を設定する。

また、ポリシー管理手段102は、ポリシー管理データベース110のネットワーク機器管理データ構造（図16参照）に基づき、ネットワーク運用者によって指定されたマルチポリシールールの適用対象のネットワーク機器に対応するネットワーク機器情報として、ネットワーク機器IDに「172.27.1.1」、インタフェースIDに「172.27.50.1」、ポリシールールへのヘッダポインタ（Link Header）にインスタンス110-P3、ポリシールールへのテールポインタ（L

ink Tail) にインスタンス 110-P3 のインスタンス 110-N1 を生成し、ポリシー管理データベース 110 内の管理情報を更新する (図 7 中の S10206, S10207)。

ポリシー管理手段 102 は、ネットワーク機器に対して登録のあるポリシールールの場合、ネットワーク機器情報としてのネットワーク機器 ID「172.27.1.1」及びインタフェース ID「172.27.50.1」と、ポリシー情報としての「ポリシールール 11」とをポリシー分析手段 201 に通知する (図 7 中の S10208)。

この通知を受けたポリシー分析手段 201 は、図 8 における処理フロー (S20101～S20104) に示すように、通知されたポリシー情報の分析を行い、ポリシー分析データベース 210 のポリシールール管理データ構造 (図 17 参照) に基づき、ポリシー名に「ポリシールール 11」、ポリシー種別に「マルチポリシー」、コンディションに「ブランク」、アクションに「ブランク」のインスタンス 210-P3 を生成し、ポリシールールとしてポリシー分析データベース 210 に格納する。

また、ポリシー分析手段 201 は、「ポリシールール 11」を構成する 2 つのシングルポリシールール「ポリシールール 1」及び「ポリシールール 3」を「ポリシールール 11」の配下に設定するために、ポリシー分析データベース 210 のマルチポリシー配下管理データ構造 (図 17 参照) に基づき、「ポリシールール 1」の場合は、ポリシー名に「ポリシールール 1」、ポリシー種別に「シングルポリシー」、コンディションに「条件 1」、アクションに「動作 1」のインスタンス 210-P3-1 を生成し、「ポリシールール 3」の場合は、ポリシー名に「ポリシールール 3」、ポリシー種別に「シングルポリシー」、コンディションに「条件 2」、アクションに「動作 2」のインスタンス 210-P3-2 を生成する。そして、ポリシー分析手段 201 は、更にインスタンス 210-P3 の次ポインタ (Next Policy) にインスタンス 210-P3-1 を、かつインスタンス 210-P3-1 の次ポインタにインスタンス 210-P3-2 をそれぞれ設定する。

次に、ポリシー分析手段 201 は、ポリシー分析データベース 210 のネットワーク機器管理データ構造 (図 17 参照) に基づき、ネットワーク機器 ID に「172.27.1.1」、インタフェース ID に「172.27.50.1」、適用ポリシー

ルール数に「0」、ポリシールールへのヘッダポインタ (Link Header) に「インスタンス210-P3」、ポリシールールへのテールポインタ (Link Tail) にインスタンス210-P3の「インスタンス210-N1」を生成し、ポリシー分析データベース210へ格納する。

ポリシー分析手段201は、ネットワーク運用状況の情報収集対象としてのネットワーク機器のネットワーク機器情報（ここでは、ネットワーク機器ID「172. 27. 1. 1」、インタフェースID「172. 27. 50. 1」）をネットワーク運用情報収集手段301へ通知する。

この通知を受けたネットワーク運用情報収集手段301は、ネットワーク管理データベース310のネットワーク管理データ構造（図18参照）に基づき、ネットワーク運用者によって指定されたマルチポリシールールの適用対象のネットワーク機器に対応する情報として、ネットワーク機器IDに「172. 27. 1. 1」、インタフェースIDに「172. 27. 50. 1」、ポート状態（回線の状態）に「0（正常）」、トラヒック量（該当インタフェースのトラヒック量）に「0」、パケットロス量（該当インタフェースのパケットロス量）に「0」のインスタンス310-N1を生成し、ネットワーク管理データベース310へ格納する（図9中のS30101, S30102）。

ネットワーク監視手段302は、図10における処理フロー（S30201～S30203）に示すように、定期的にネットワーク管理データベース310を参照し、ネットワーク運用状況を収集する必要があるネットワーク機器情報があれば、対象のネットワーク機器から図示省略の通信インタフェース手段を介してネットワーク運用状況（つまり、回線の状態（ポートの状態）、トラヒック量、パケットロス量）を取得する。この例では、172. 27. 1. 1がネットワーク機器情報として設定されているため、ネットワーク監視手段302は、172. 27. 1. 1対応のネットワーク機器からネットワーク運用状況（ここでは、回線状態が「障害」、トラヒック量が「0」、パケットロス量が「0」とする）を取得する。ネットワーク監視手段302は、取得したネットワーク運用状況を参照して、ネットワーク管理データベース310のネットワーク管理データ構造（図18参照）に従い、インスタンス310-N1のポート状態に「1（障害）」、トラヒック量に「0」、パケットロス量に「0」

をそれぞれ設定し、ネットワーク管理データベース 310 の情報を更新する。

図 5 に示すように、ネットワーク運用情報収集手段 301 は、ネットワーク管理データベース 310 を参照し、ネットワーク運用状況の情報に変化があるかを監視する（図 9 中の S30103）。この例では、インスタンス 310-N1 のポート状態が障害に変化したため、ネットワーク機器情報としてのネットワーク機器 ID「172.27.1.1」及びインタフェース ID「172.27.50.1」と、ネットワーク運用状況の情報としての回線の状態「障害」、トラヒック量「0」及びパケットロス量「0」をネットワーク状況分析手段 303 へ通知する（図 9 中の S30104, S30105）。

この通知を受けたネットワーク状況分析手段 303 は、図 11 における処理フロー（S30301～S30305）に示すように、通知されたネットワーク運用状況の情報を分析し、ネットワーク機器情報（ネットワーク機器 ID「172.27.1.1」及びインタフェース ID「172.27.50.1」）と、このネットワーク機器の運用状況（回線の状態「障害」、トラヒック量「0」、パケットロス量「0」）とを抽出し、抽出した情報を最適ポリシー選択手段 304 へポリシー適用要求として通知する。

最適ポリシー選択手段 304 は、図 12 における処理フロー（S30401～S30406）に示すように、通知されたネットワーク機器情報のネットワーク機器 ID「172.27.1.1」及びインタフェース ID「172.27.50.1」に基づき、ポリシー分析データベース 210 より、このネットワーク機器に対応して登録されているポリシールールの一覧を抽出する。そして、最適ポリシー選択手段 304 は、抽出したポリシールールの一覧より、最適なポリシールールを選択（決定）する。この例では、このネットワーク機器に対しては、マルチポリシールールとしての「ポリシールール 11」が登録されているので、最適ポリシー選択手段 304 は選択した「ポリシールール 11」をポリシー適用指示手段 305 へ通知する。

ポリシー適用指示手段 305 は、図 13 における処理フロー（S30501～S30506）に示すように、通知された「ポリシールール 11」を分析し、ポリシールール（マルチポリシールール）内の各アクションを行う、つまりシングルポリシールールが無くなる迄、処理を繰り返す。この例では、マルチポリシールールとして「ポ

リシールール1」及び「ポリシールール3」が処理対象となる。「ポリシールール1」におけるアクションはルート2への経路切替となっているため、ポリシー適用指示手段305はポリシー適用手段306に対してネットワーク機器ID「172.27.1.1」のネットワーク機器へのポリシー適用を要求する。

要求を受けたポリシー適用手段306は、図14における処理フロー（S30601～S30602）に示すように、適用対象のネットワーク機器に対して、トラヒックの流れる経路をルート1からルート2に変更するように制御する。

また、「ポリシールール3」におけるアクションはネットワーク運用者へのメール通知となっているため、ポリシー適用指示手段305は関連処理実行手段307へ処理を要求する。

要求を受けた関連処理実行手段307は、図15における処理フロー（S30701～S30702）に示すように、ネットワーク運用者が利用するメールアドレス「pserver@xyz.com」に対して、回線が障害である旨の通知をメールする。ポリシー適用手段306へのポリシー適用要求後、ポリシー適用指示手段305はポリシー分析データベース210の該当ポリシールールの適用状態を「適用」に設定する。

なお、ポリシー適用手段306及び関連処理実行手段307は図示省略の通信インタフェース手段を介してIPネットワーク3に接続される。

〈第2の動作例〉

第2の動作例のポリシールール適用ネットワークシステム1においては、同一コンディションのシングルポリシールールに運用用途に応じた優先順位（優先度）を付与し、その優先順位に従って適用することにより、多様化し瞬時に状況が変遷していくIPネットワーク3を柔軟に制御することを可能にしている。

図4に示すように、ネットワーク運用者は、ポリシーサーバ2に接続される保守・運用端末を利用して、コンディションとして、ユーザ端末Xからユーザ端末Yへルート1で流れるトラヒック（IPフロー）に対して閾値を40%とする回線単位のトラヒック量閾値超過時「条件4」、アクションとして、ユーザ端末Xからユーザ端末Yへルート2で流れる様に経路切替「動作4」を行う「ポリシールール4」を指定し、ユーザインタフェース手段101を介してポリシールールの登録要求を行う（図6中

のS10101, S10102)。

同様に、ネットワーク運用者は、コンディションとして、ユーザ端末Xからユーザ端末Yへルート1で流れるトラヒックに対して閾値を40%とする回線単位のトラヒック量閾値超過時「条件5」(条件4と同一)、アクションとして、ユーザ端末Xからユーザ端末Yへ流れるトラヒックを抑制するフロー制御「動作5」を行う「ポリシールール5」を指定し、ユーザインタフェース手段101を介してポリシールールの登録要求を行う(図6中のS10101, S10102)。

これらのポリシールールの登録要求を受けたポリシー管理手段102は、ポリシー管理データベース110のポリシールール管理データ構造(図16参照)に基づき、「ポリシールール4」の場合、ポリシー名に「ポリシールール4」、ポリシー種別に「シングルポリシー」、コンディションに「条件4」、アクションに「動作4」のインスタンス110-P4を生成し、かつ「ポリシールール5」の場合、ポリシー名に「ポリシールール5」、ポリシー種別に「シングルポリシー」、コンディションに「条件5」、アクションに「動作5」のインスタンス110-P5を生成し、ポリシールールとしてポリシー管理データベース101へ格納する(図7中のS10201~S10203)。

次に、ネットワーク運用者は、ポリシールール4の優先度を「低」とし、かつポリシールール5の優先度を「高」とする、つまり同一コンディションで異なるアクションになるように、ポリシールールの優先順位付けを行い、この優先度付けポリシールールの適用対象のネットワーク機器を指定することにより、ユーザインタフェース手段101を介して優先度付けポリシールール(シングルポリシールール)の登録要求が行える(図6中のS10101~S10102)。ここでは、優先度付けポリシールールの適用対象のネットワーク機器がノード4に対応するネットワーク機器Aであるので、ネットワーク運用者はネットワーク機器ID「172.27.1.1」及びインタフェースID「172.27.50.1」を指定する。なお、優先度は高・低の2種類に限定されず、高・中・低など3種類以上を適用してもよい。

この優先度付けポリシールールの登録要求を受けたポリシー管理手段102は、インスタンス110-P4の優先順位に「低」、インスタンス110-P4の次ポインタ(Next Policy)にインスタンス100-P5、かつインスタンス11

0-P5の優先順位に「高」をそれぞれ設定し、ポリシー管理データベース110を更新する(図7中のS10209, S10210)。

また、ポリシー管理手段102は、ポリシー管理データベース110のネットワーク機器管理データ構造(図16参照)に基づき、ネットワーク運用者によって指定された優先度付けポリシールールの適用対象のネットワーク機器に対応するネットワーク機器情報として、ネットワーク機器IDに「172. 27. 1. 1」、インタフェースIDに「172. 27. 50. 1」、ポリシールールへのヘッダポインタ(Link Header)にインスタンス110-P4、かつポリシールールへのテールポインタ(Link Tail)にインスタンス110-P5のインスタンス110-N2を生成し、ポリシー管理データベース110内の管理情報を更新する(図7中のS10206, S10207)。

ポリシー管理手段102は、ネットワーク機器に対して登録のあるポリシールールの場合、ネットワーク機器情報としてのネットワーク機器ID「172. 27. 1. 1」及びインタフェースID「172. 27. 50. 1」と、ポリシー情報としての「ポリシールール4」及び「ポリシールール5」とをポリシー分析手段201に通知する(図7中のS10208)。

この通知を受けたポリシー分析手段201は、図8における処理フロー(S20101~S20104)に示すように、通知されたポリシー情報の分析を行い、ポリシー分析データベース210のポリシールール管理データ構造(図17参照)に基づき、「ポリシールール4」の場合、ポリシー名に「ポリシールール4」、ポリシー種別に「シングルポリシー」、コンディションに「条件4」、アクションに「動作4」、優先順位に「低」のインスタンス210-P4を生成し、かつ「ポリシールール5」の場合、ポリシー名に「ポリシールール5」、ポリシー種別に「シングルポリシー」、コンディションに「条件5」、アクションに「動作5」、優先順位に「高」のインスタンス210-P5を生成し、ポリシー分析データベース210へ格納する。

次に、ポリシー分析手段201は、ポリシー分析データベース210のネットワーク管理データ構造(図17参照)に基づき、ネットワーク機器IDに「172. 27. 1. 1」、インタフェースIDに「172. 27. 50. 1」、適用ポリシールール数に「0」、ポリシールールへのヘッダポインタ(Link Header)にイン

スタンス 210-P4、ポリシールールへのテールポインタ (Link Tail) にインスタンス 210-P5 のインスタンス 210-N2 を生成し、ポリシー分析データベース 210 へ格納する。

ポリシー分析手段 201 は、ネットワーク運用状況の情報収集対象としてのネットワーク機器のネットワーク機器情報 (ここでは、ネットワーク機器 ID 「172. 27. 1. 1」、インタフェース ID 「172. 27. 50. 1」) を監視ポイントとしてネットワーク運用情報収集手段 301 へ通知する。

この通知を受けたネットワーク運用情報収集手段 301 は、ネットワーク管理データベース 310 のネットワーク管理データ構造 (図 18 参照) に基づき、ネットワーク運用者によって指定された優先度付けポリシールールの適用対象のネットワーク機器に対応する情報として、ネットワーク機器 ID に「172. 27. 1. 1」、インタフェース ID に「172. 27. 50. 1」、ポート状態 (回線の状態) に「0 (正常)」、トラヒック量 (該当インタフェースのトラヒック量) に「0」、パケットロス量 (該当インタフェースのパケットロス量) に「0」のインスタンス 310-N1 を生成し、ネットワーク管理データベース 310 へ格納する (図 9 中の S30101, S30102)。

ネットワーク監視手段 302 は、図 10 における処理フロー (S30201, S30202) に示すように、定期的にネットワーク管理データベース 310 を参照し、ネットワーク運用状況を収集する必要があるネットワーク機器情報があれば、対象のネットワーク機器から図示省略の通信インタフェース手段を介してネットワーク運用状況 (つまり、回線の状態 (ポート状態)、トラヒック量、パケットロス量) を取得する。この例では、172. 27. 1. 1 がネットワーク機器情報として設定されているため、ネットワーク監視手段 302 は、172. 27. 1. 1 対応のネットワーク機器からネットワーク運用状況 (ここでは、回線状態が「通常」、トラヒック量が「50Mbps」、パケットロス量が「0」とし、インタフェースの物理帯域を「100Mbps」とする) を取得する。ネットワーク監視手段 302 は、取得したネットワーク運用状況を参照して、ネットワーク管理データベース 310 のネットワーク管理データ構造 (図 18 参照) に従い、インスタンス 310-N2 のポート状態に「0 (通常)」、トラヒック量に「50Mbps」、パケットロス量に「0」をそれぞれ

設定し、ネットワーク管理データベース 310 の情報を更新する。

図 5 に示すように、ネットワーク運用情報収集手段 301 は、ネットワーク管理データベース 310 を参照し、ネットワーク運用状況の情報に変化があるかを監視する（図 9 中の S30103）。この例では、インスタンス 310-N2 のトラフィック量が増加したため、ネットワーク機器情報としてのネットワーク機器 ID「172.27.1.1」及びインタフェース ID「172.27.50.1」と、ネットワーク運用状況の情報としての回線の状態「通常」、トラフィック量「50Mbps」、パケットロス量「0」をネットワーク状況分析手段 303 へ通知する（図 9 中の S30104, S30105）。

この通知を受けたネットワーク分析 303 は、図 11 における処理フロー（S30301～S30305）に示すように、通知されたネットワーク運用状況の情報を分析し、ネットワーク機器情報（ネットワーク機器 ID「172.27.1.1」及びインタフェース ID「172.27.50.1」）と、このネットワーク機器の運用状況（回線の状態「通常」、トラフィック量「50Mbps」、パケットロス量「0」）を抽出し、抽出した情報を最適ポリシー選択手段 304 へポリシー適用要求として通知する。

最適ポリシー選択手段 304 は、図 12 における処理フロー（S30401～S30406）に示すように、通知されたネットワーク機器情報のネットワーク機器 ID「172.27.1.1」及びインタフェース ID「172.27.50.1」に基づき、ポリシー分析データベース 210 より、このネットワーク機器に対応して登録されているポリシールールの一覧を抽出する。そして、最適ポリシー選択手段 304 は、抽出したポリシールールの一覧より、優先順位に従って最適なポリシールールを選択（決定）する。この例では、物理帯域 100Mbps に対してトラフィック量が 50Mbps であるため、割合が 50% となり、トラフィック量超過の閾値である 40% を超えていると、最適ポリシー選択手段 304 は判断する。したがって、ネットワーク機器には、シングルポリシールールとしての「ポリシールール 4」及び「ポリシールール 5」が登録されており、「ポリシールール 5」の優先順位が「高」であるため、「ポリシールール 5」が選択される。最適ポリシー選択手段 304 は選択した「ポリシールール 5」をポリシー適用指示手段 305 へ通知する。

ポリシー適用指示手段 305 は、図 13 における処理フロー（S30501～S30505）に示すように、通知された「ポリシールール 5」を分析し、ポリシールール（マルチポリシールール）内の各アクションを行う、つまりシングルポリシールールが無くなる迄、処理を繰り返す。この例では、「ポリシールール 5」は、シングルポリシールールであり、アクションとしては、1つであるため、このアクションのみが処理の対象となる。「ポリシールール 5」は、アクションとして、ユーザ端末 X からユーザ端末 Y へのトラヒックを抑制するフロー制御となっているため、ポリシー適用指示手段 305 はポリシー適用手段 306 に対してネットワーク機器 ID「172.27.1.1」のネットワーク機器へのポリシー適用を要求する。

要求を受けたポリシー適用手段 306 は、図 14 における処理フロー（S30601, S30602）に示すように、適用対象のネットワーク機器に対して、フロー制御を行う。ポリシー適用手段 306 へのポリシー適用要求後、ポリシー適用指示手段 305 はポリシー分析データベース 210 の該当ポリシールールの適用状態を「適用」に設定する。

〈第 3 の動作例〉

上述した第 2 の動作例に代替して、ネットワーク運用者は、ポリシーサーバ 2 に接続される保守・運用端末を利用し、複数種類の優先度（例えば、最高、高、中、低）を割り当てたマルチポリシールールを作成する。例えば、図 2（A），（B）に示すように、「回線単位障害発生」に関する同一コンディションに属するシングルポリシールール 1, 2, 3 を組み合わせたマルチポリシールール 10, 11, 12, 13 については、優先度を「低」、「高」、「最高」、「中」にそれぞれ割り当てる。

ネットワーク運用者は、更にこの優先度付けマルチポリシールールを適用するネットワーク機器（例えば、ネットワーク機器 ID が「172.27.1.1」及びインタフェース ID が「172.27.50.1」のネットワーク機器）を指定する。

これにより、ユーザインタフェース手段 101 を介してポリシー管理手段 102 にポリシールールの登録要求が行われる。この結果、上述した第 2 の動作例における優先度付けシングルポリシールールの適用と同様に、優先度付けマルチポリシールールについても優先度を用いたポリシー適用が行える。

この第 3 の動作例のポリシールール適用ネットワークシステム 1 においては、同一

コンディションに属する複数のシングルポリシールールを組み合わせた複数のマルチポリシールールに優先順位を付与して適用することにより、付加価値を有するIPネットワーク3に一層柔軟に対応することが可能になる。

〈第4の動作例〉

第4の動作例のポリシールール適用ネットワークシステム1においては、マルチポリシールール内の複数のシングルポリシールールに優先順位を付与することにより、付加価値を有するIPネットワーク3に一層柔軟に対応することを可能にしている。

上述した第1の動作例に代替して、ネットワーク運用者は、ポリシーサーバ2に接続される保守・運用端末を利用し、図2(C)に示すように、例えばマルチポリシールールである「ポリシールール11」内の2つのシングルポリシールールの「ポリシールール1」及び「ポリシールール3」に「低」及び「高」の優先順位付けを行い、「ポリシールール11」を適用するネットワーク機器（例えば、ネットワーク機器IDが「172.27.1.1」及びインタフェースIDが「172.27.50.1」のネットワーク機器）を指定する。これにより、ユーザインタフェース手段101を介してポリシー管理手段102にポリシールールの登録要求が行われる。

登録要求を受けたポリシー管理手段102は、上述した第1の動作例との差分として、インスタンス110-P3-1の優先順位に「低」を、かつインスタンス110-P3-2の優先順位に「高」を設定する。

また、ポリシー分析手段201は、上述した第1の動作例との差分として、インスタンス210-P3-1の優先順位に「低」を、かつインスタンス210-P3-2の優先順位に「高」を設定する。

さらに、ポリシー適用指示手段305は、上述した第1の動作例との差分として、マルチポリシールール内のシングルポリシールールの優先順位に従い、「ポリシールール3」、「ポリシールール1」の順番に適用処理を行う。適用処理後、ポリシー適用指示手段305はポリシー分析データベース210の該当ポリシールールの適用状態を「適用」に設定する。

〔変形例〕

上述した一実施の形態における処理はコンピュータで実行可能なプログラムとして提供され、CD-ROMやフレキシブルディスクなどの記録媒体、さらには通信回線

を経て提供可能である。

また、上述した一実施の形態における各処理はその任意の複数または全てを選択し組合せて実施することもできる。

産業上の利用可能性

シングルポリシールールが運用に伴って単調に増大することを抑制可能にしたり、ネットワーク運用者の負担を格段に減少させることを可能にするこの発明によるポリシールール適用ネットワークシステムは、ポリシーサーバにより運用されるMPLSネットワーク等のIPネットワークに適用可能である。

請求の範囲

1. 管理対象ネットワークの運用状況の変遷に応じて、前記ネットワーク内に存在する個々のネットワーク機器の動作設定のために、コンディションとこれに対応するアクションとにより規定されるポリシールールを反映させるポリシー制御装置であって；

同一コンディションで異なるアクションのシングルポリシールールの少なくとも2つを組み合わせ単位として生成された複数のマルチポリシールールを適用対象ネットワーク機器の特定情報とともに更新可能に格納する記憶手段と；

この記憶手段に格納されている前記複数のマルチポリシールールのいずれかを前記特定情報に基づいて識別した前記ネットワーク機器の動作設定のために適用する制御手段と；

を備えるポリシー制御装置。

2. 管理対象ネットワークの運用状況の変遷に応じて、前記ネットワーク内に存在する個々のネットワーク機器の動作設定のために、コンディションとこれに対応するアクションとにより規定されるポリシールールを反映させるポリシー制御装置であって；

同一コンディションで異なるアクションの複数のシングルポリシールールを適用対象ネットワーク機器の特定情報及び適用優先度情報とともに更新可能に格納する記憶手段と；

前記優先度情報に基づく優先順位で、前記記憶手段に格納されている前記複数のシングルポリシールールのいずれかを前記特定情報に基づいて識別した前記ネットワーク機器の動作設定のために適用する制御手段と；

を備えるポリシー制御装置。

3. 前記コンディションは、前記管理対象ネットワークの運用状況を示す、回線障害、トラヒック量閾値超過、及びパケットロス量閾値超過の少なくとも1つを含み、

前記アクションは、トラヒックの流れる経路の切替、トラヒックを抑制するためのフロー制御、及びネットワーク運用者への通知の少なくとも2つを含む

請求項 1 または 2 記載のポリシー制御装置。

4. 前記適用対象ネットワーク機器の特定情報は、前記ネットワーク機器の識別情報及び回線インタフェースの識別情報を含む

請求項 1 または 2 記載のポリシー制御装置。

5. 前記複数のマルチポリシールールそれぞれの、前記ポリシールールの階層的管理を可能にするために、前記記憶手段に予め登録された同一コンディションで異なるアクションの前記シングルポリシールールの少なくとも 2 つを組み合わせ単位として生成される

請求項 1 記載のポリシー制御装置。

6. 前記記憶手段は、更に前記複数のマルチポリシールールの適用優先度情報を更新可能に格納し、

前記制御手段は、前記優先度情報に基づく優先順位で前記複数のマルチポリシールールのいずれかを前記ネットワーク機器の動作設定のために適用する

請求項 1 記載のポリシー制御装置。

7. 前記記憶手段は、更に前記複数のマルチポリシールールのそれぞれ内の前記シングルポリシールールの適用優先度情報を更新可能に格納し、

前記制御手段は、前記優先度情報に基づく優先順位で前記複数のマルチポリシールールのそれぞれ内の前記シングルポリシールールを前記ネットワーク機器の動作設定のために適用する

請求項 1 記載のポリシー制御装置。

8. 管理対象ネットワークの運用状況の変遷に応じて、前記ネットワーク内に存在する個々のネットワーク機器の動作設定のために、コンディションとこれに対応するアクションとにより規定されるポリシールールを反映させるポリシー制御方法であって；

同一コンディションで異なるアクションのシングルポリシーールの少なくとも2つを組み合わせ単位として生成された複数のマルチポリシーールを適用対象ネットワーク機器の特定情報とともに更新可能に格納し；

格納されている前記複数のマルチポリシーールのいずれかを前記特定情報に基づいて識別した前記ネットワーク機器の動作設定のために適用する；

ポリシー制御方法。

9. 管理対象ネットワークの運用状況の変遷に応じて、前記ネットワーク内に存在する個々のネットワーク機器の動作設定のために、コンディションとこれに対応するアクションとにより規定されるポリシーールを反映させるポリシー制御方法であって；

同一コンディションで異なるアクションの複数のシングルポリシーールを適用対象ネットワーク機器の特定情報及び適用優先度情報とともに更新可能に格納し；

前記優先度情報に基づく優先順位で、格納されている前記複数のシングルポリシーールのいずれかを前記特定情報に基づいて識別した前記ネットワーク機器の動作設定のために適用する；

ポリシー制御方法。

10. 前記コンディションは、前記管理対象ネットワークの運用状況を示す、回線障害、トラヒック量閾値超過、及びパケットロス量閾値超過の少なくとも1つを含み、

前記アクションは、トラヒックの流れる経路の切替、トラヒックを抑制するためのフロー制御、及びネットワーク運用者への通知の少なくとも2つを含む

請求項8または9記載のポリシー制御方法。

11. 前記適用対象ネットワーク機器の特定情報は、前記ネットワーク機器の識別情報及び回線インタフェースの識別情報を含む

請求項8または9記載のポリシー制御方法。

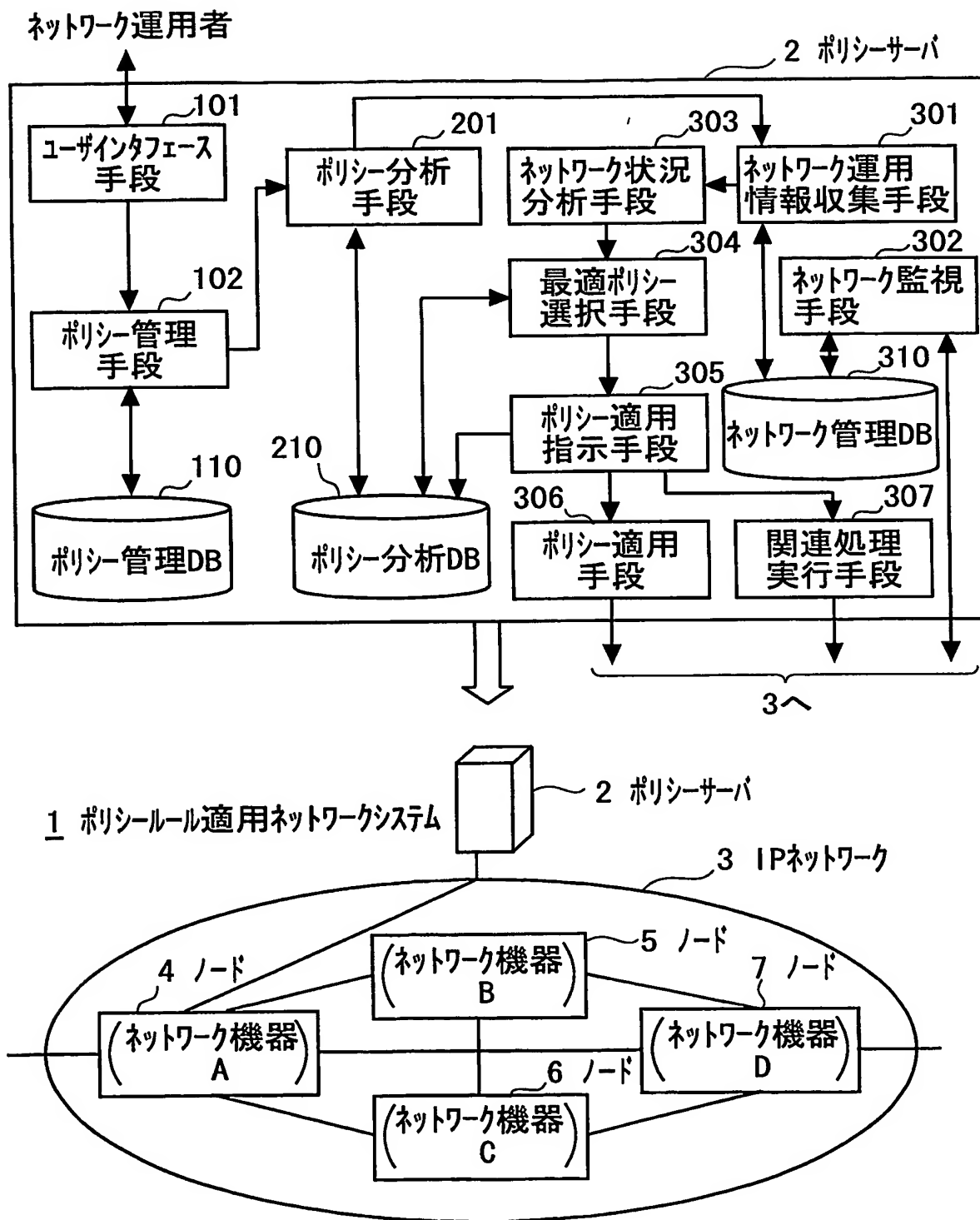
12. 前記複数のマルチポリシーールのそれぞれは、前記ポリシーールの階層

的管理を可能にするために、予め登録された同一コンディションで異なるアクションの前記シングルポリシールールของอย่างน้อย 2 つを組み合わせ単位として生成される請求項 8 記載のポリシー制御方法。

1 3. 更に前記複数のマルチポリシールールの適用優先度情報を更新可能に格納し、前記優先度情報に基づく優先順位で前記複数のマルチポリシールールのいずれかを前記ネットワーク機器の動作設定のために適用する
請求項 8 記載のポリシー制御方法。

1 4. 更に前記複数のマルチポリシールールのそれぞれ内の前記シングルポリシールールの適用優先度情報を更新可能に格納し、
前記優先度情報に基づく優先順位で前記複数のマルチポリシールールのそれぞれ内の前記シングルポリシールールを前記ネットワーク機器の動作設定のために適用する
請求項 8 記載のポリシー制御方法。

1/17
FIG. 1



2/17

FIG. 2

(A)

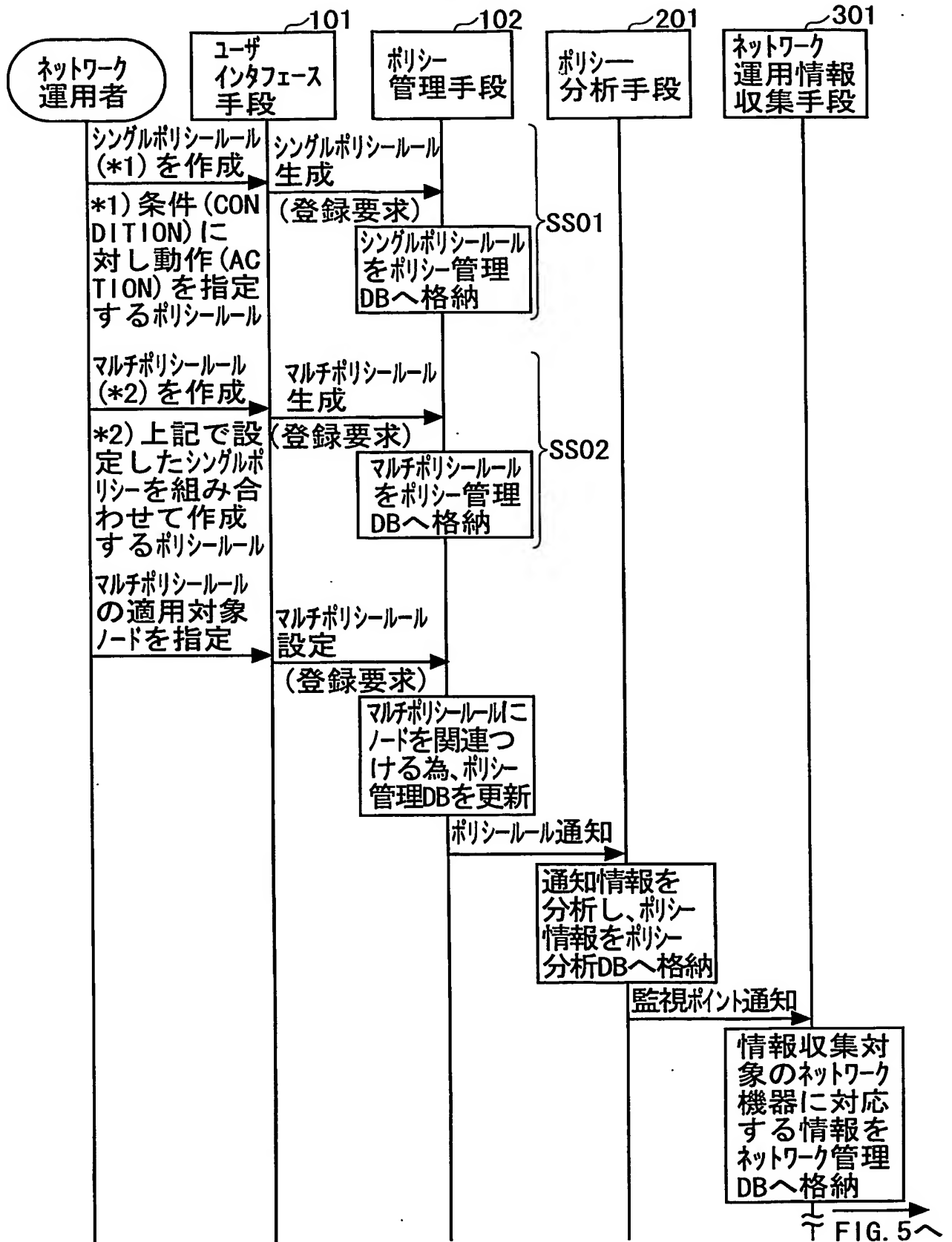
シングル ポリシールール	アクション	経路切替	フロー制御	メール通知
ポリシールール1	回線単位障害発生	●		
ポリシールール2	回線単位障害発生		●	
ポリシールール3	回線単位障害発生			●
ポリシールール4	回線単位トラフィック量閾値超過	●		
ポリシールール5	回線単位トラフィック量閾値超過		●	
ポリシールール6	回線単位トラフィック量閾値超過			●
ポリシールール7	回線単位パケットロス量閾値超過	●		
ポリシールール8	回線単位パケットロス量閾値超過		●	
ポリシールール9	回線単位パケットロス量閾値超過			●

(B)

マルチポリシールール	シングルポリシールール組み合わせ
ポリシールール10	ポリシールール①+ポリシールール②
ポリシールール11	ポリシールール①+ポリシールール③
ポリシールール12	ポリシールール②+ポリシールール③
ポリシールール13	ポリシールール①+ポリシールール②+ポリシールール③
ポリシールール14	ポリシールール④+ポリシールール⑤
ポリシールール15	ポリシールール④+ポリシールール⑥
ポリシールール16	ポリシールール⑤+ポリシールール⑥
ポリシールール17	ポリシールール④+ポリシールール⑤+ポリシールール⑥
ポリシールール18	ポリシールール⑦+ポリシールール⑧
ポリシールール19	ポリシールール⑦+ポリシールール⑨
ポリシールール20	ポリシールール⑧+ポリシールール⑨
ポリシールール21	ポリシールール⑦+ポリシールール⑧+ポリシールール⑨

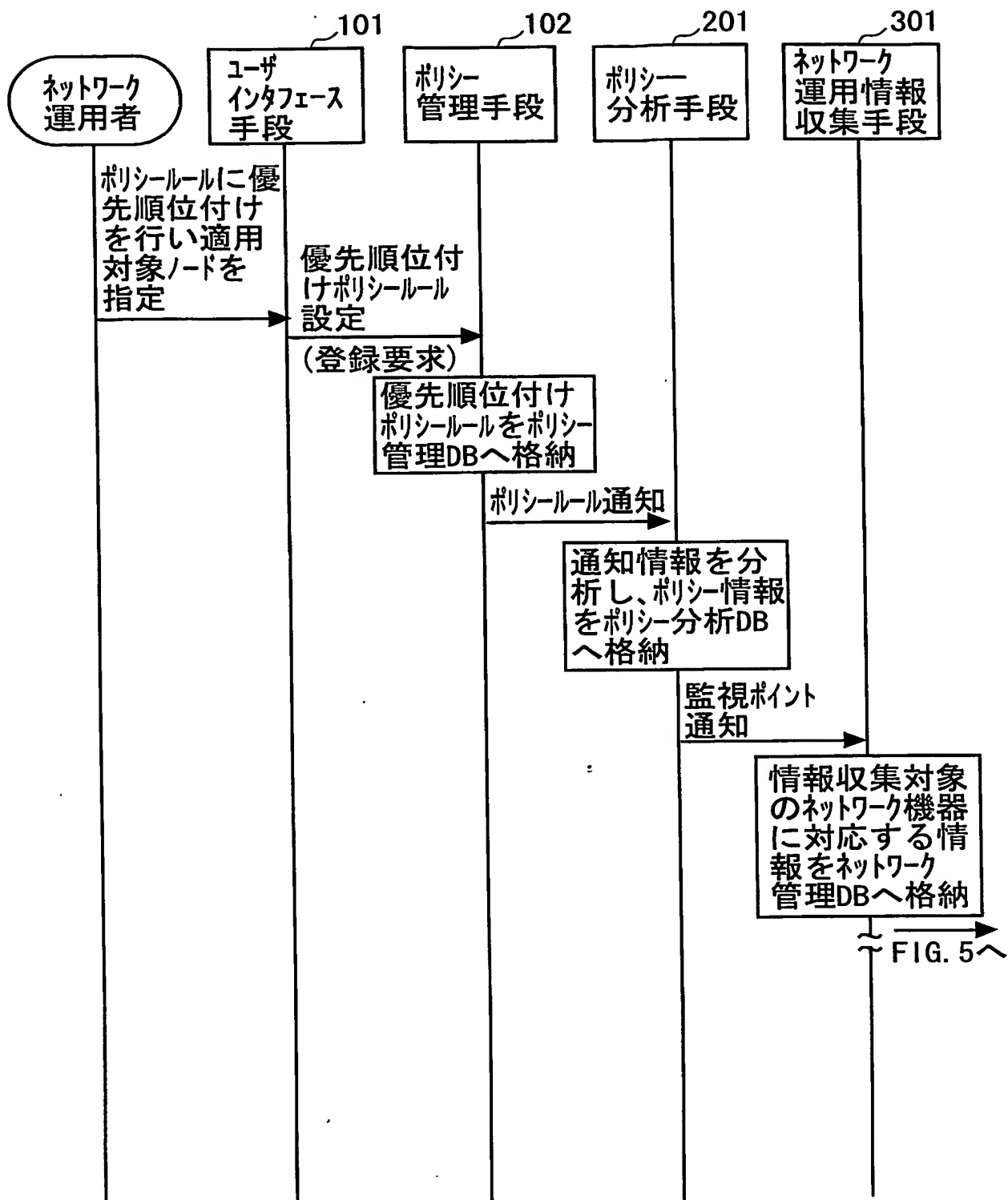
(C)

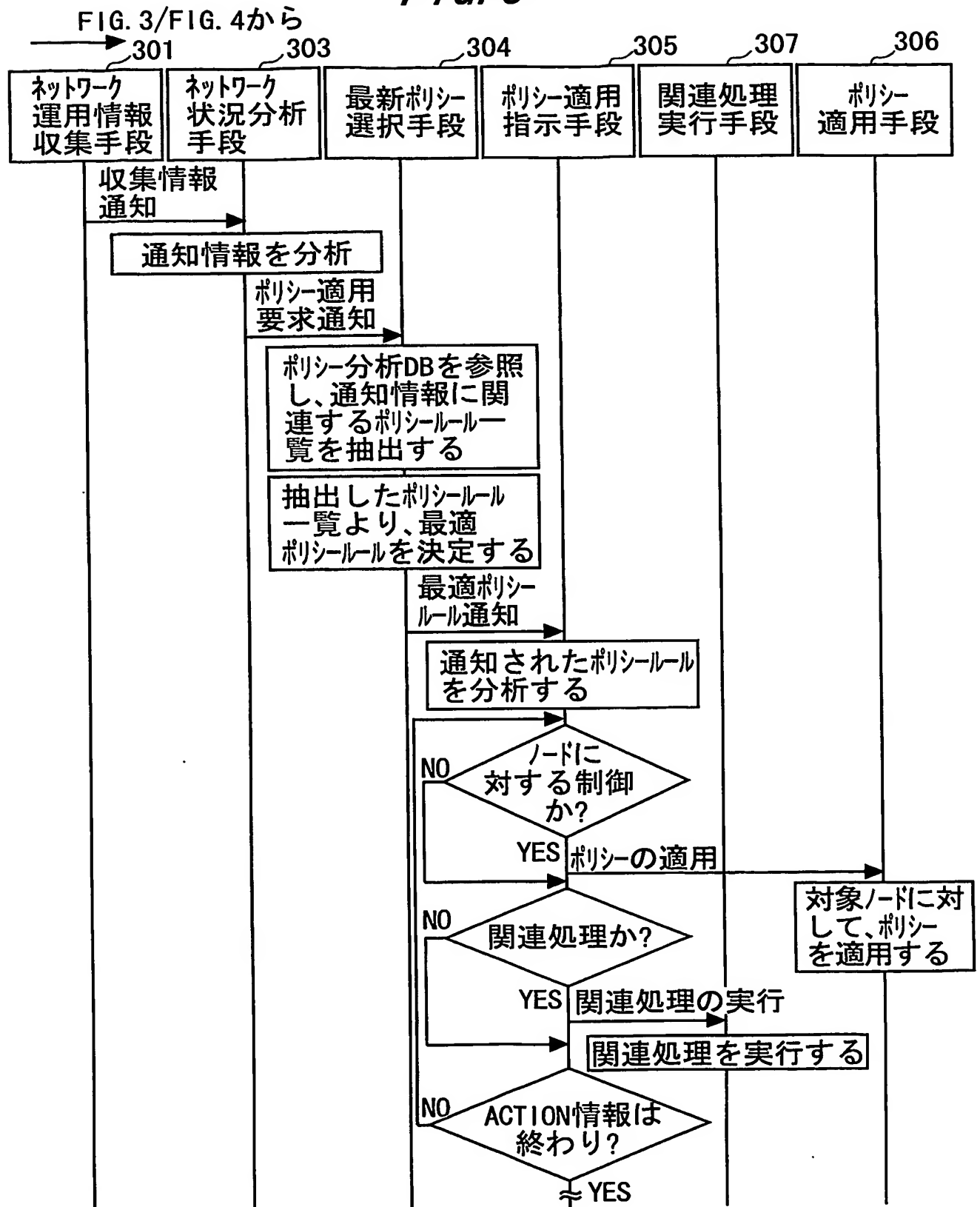
パス名	割当ポリシールール	優先度(プライオリティ)
TUNNEL-1	ポリシールール1	高
	ポリシールール2	低
TUNNEL-2	ポリシールール3	高
	ポリシールール1	低
⋮	⋮	⋮

3/17
FIG. 3

4/17

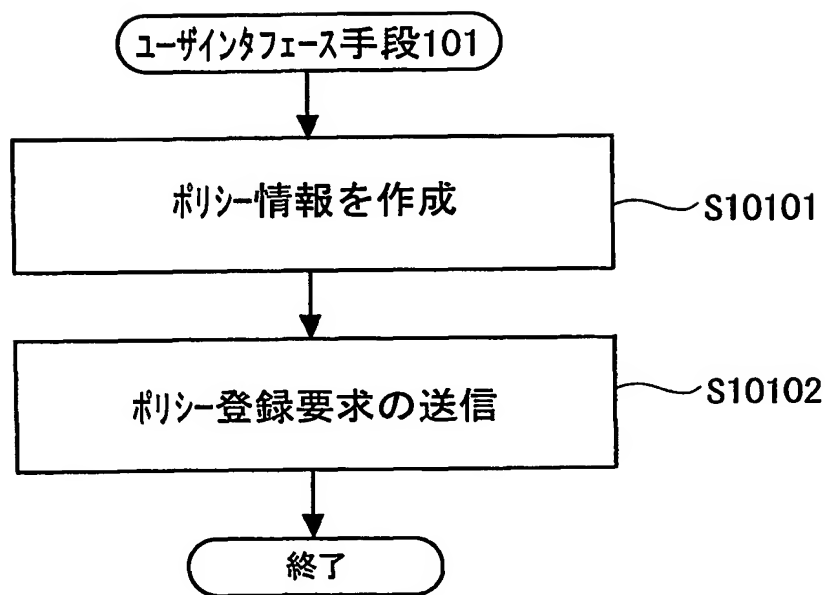
FIG. 4



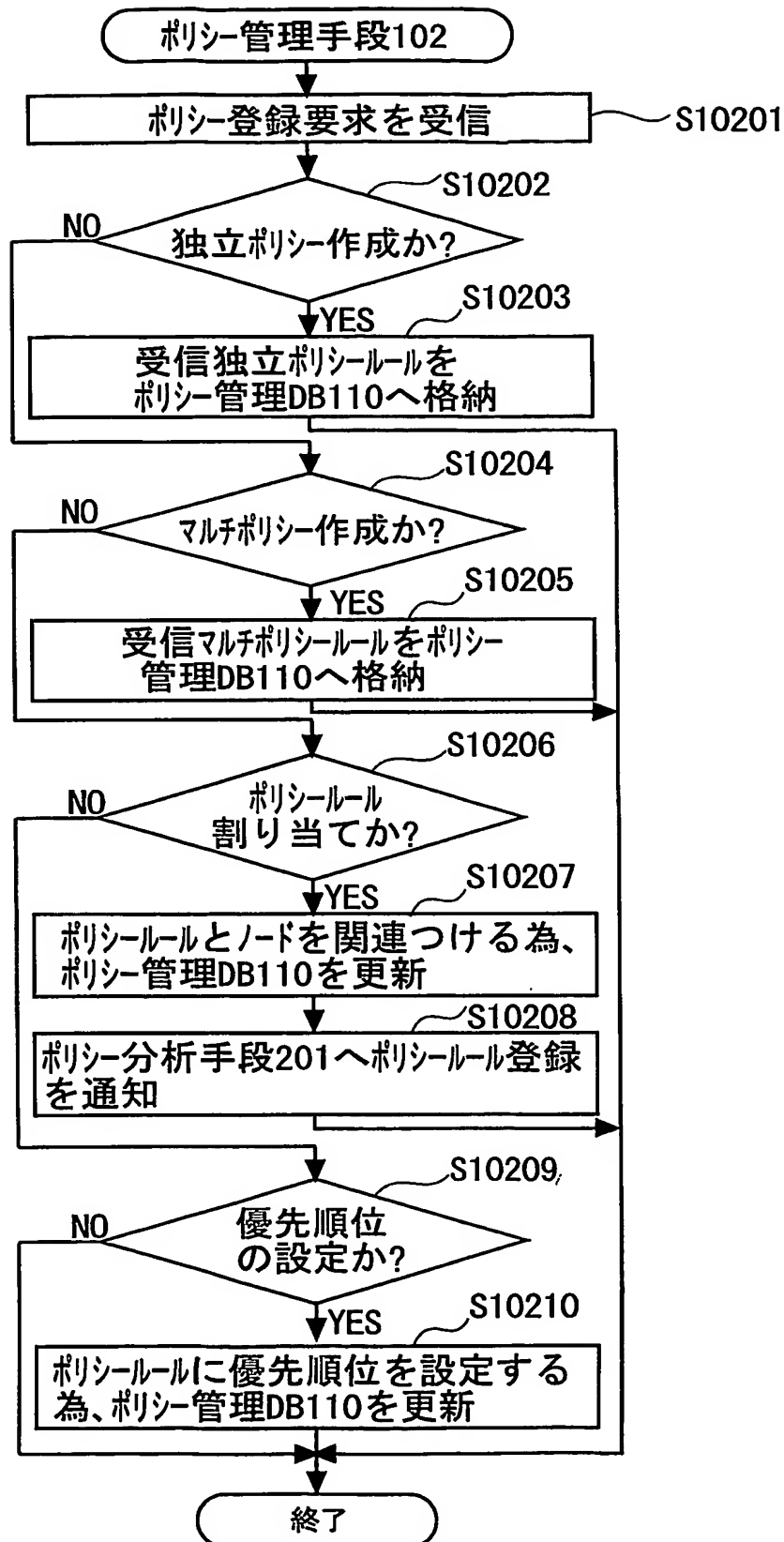
5/17
FIG. 5

6/17

FIG. 6

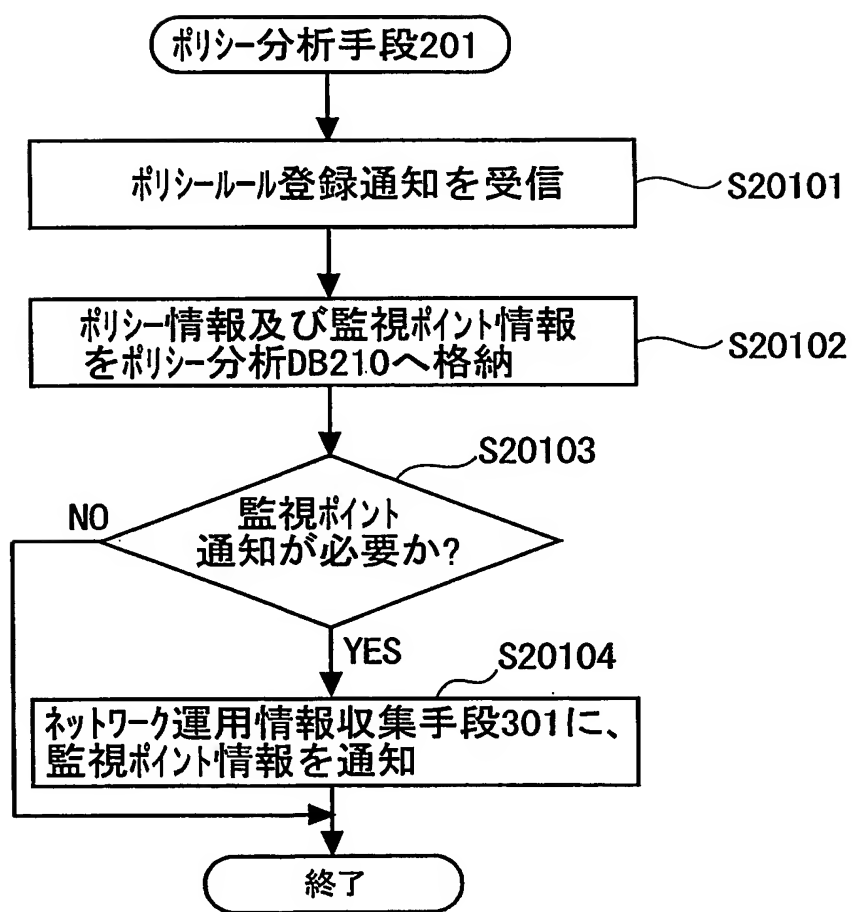


7/17
FIG. 7



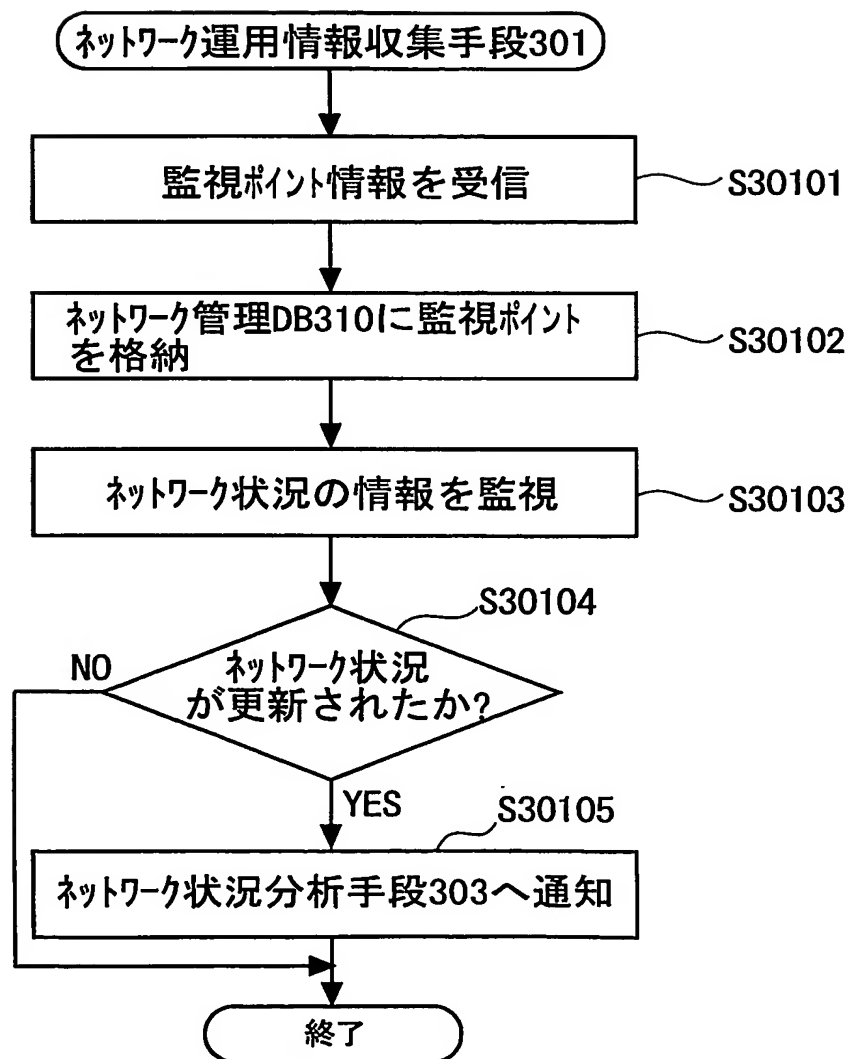
8/17

FIG. 8



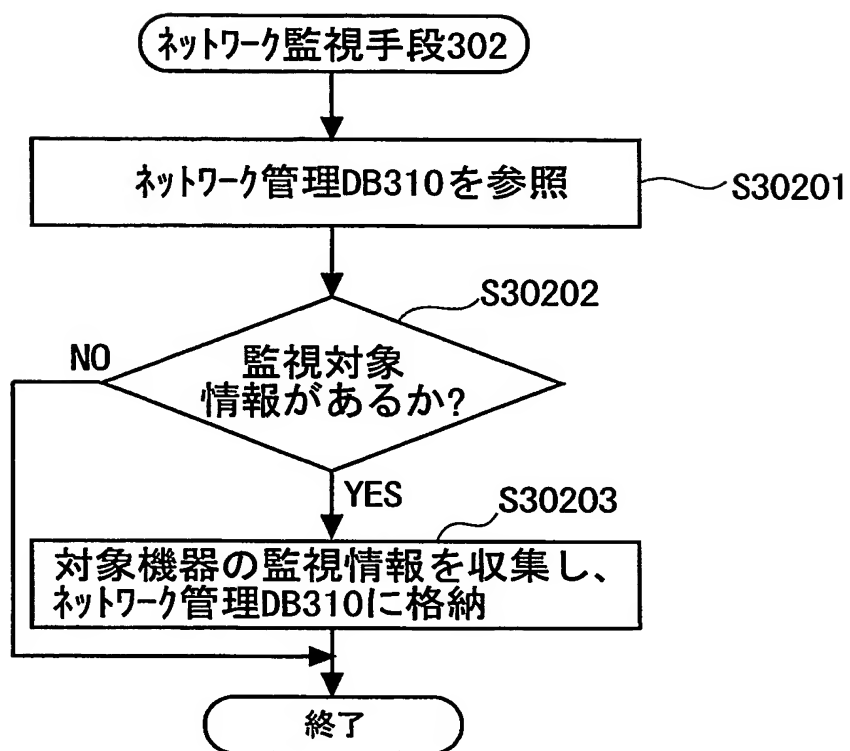
9/17

FIG. 9



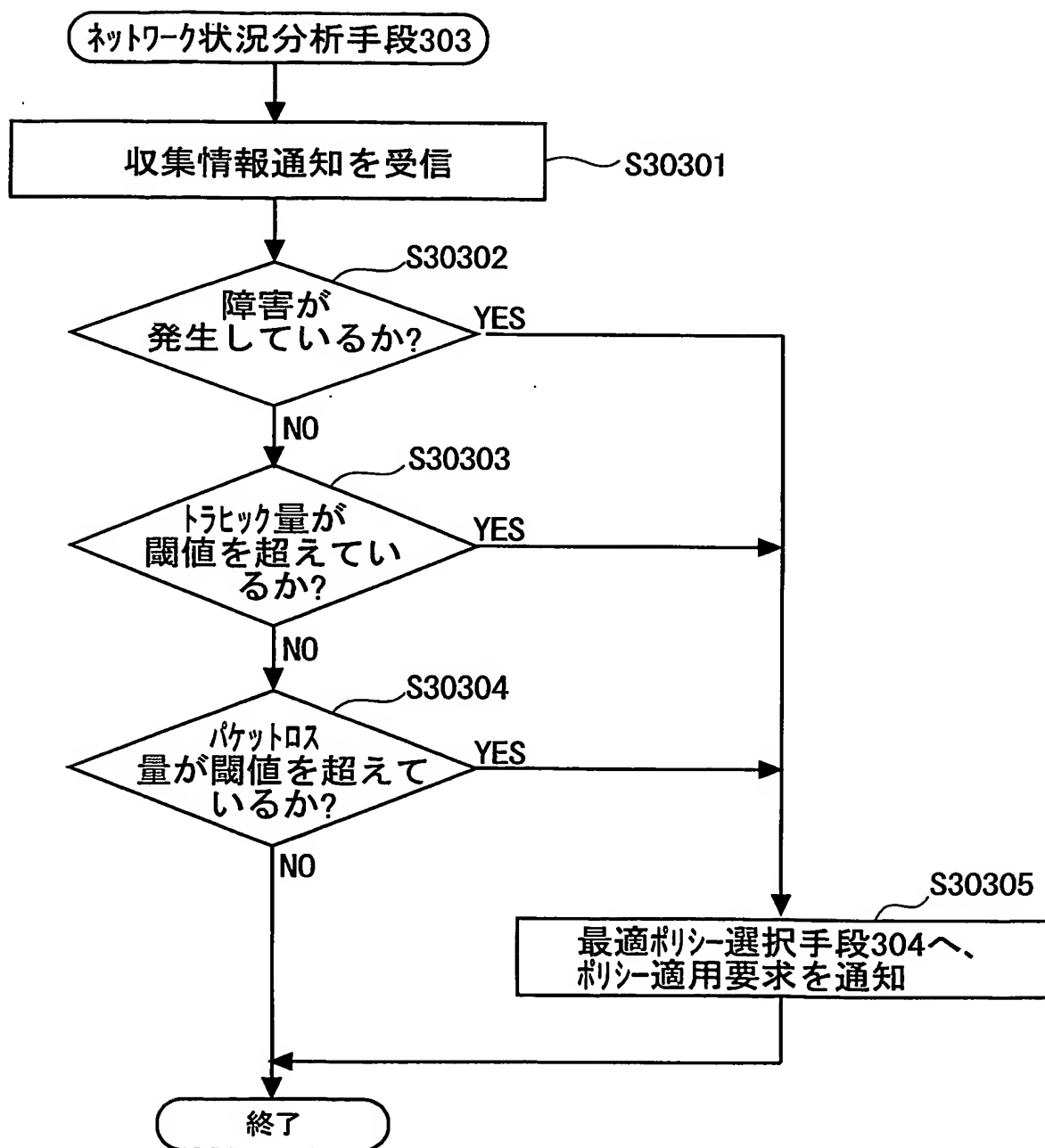
10/17

FIG. 10



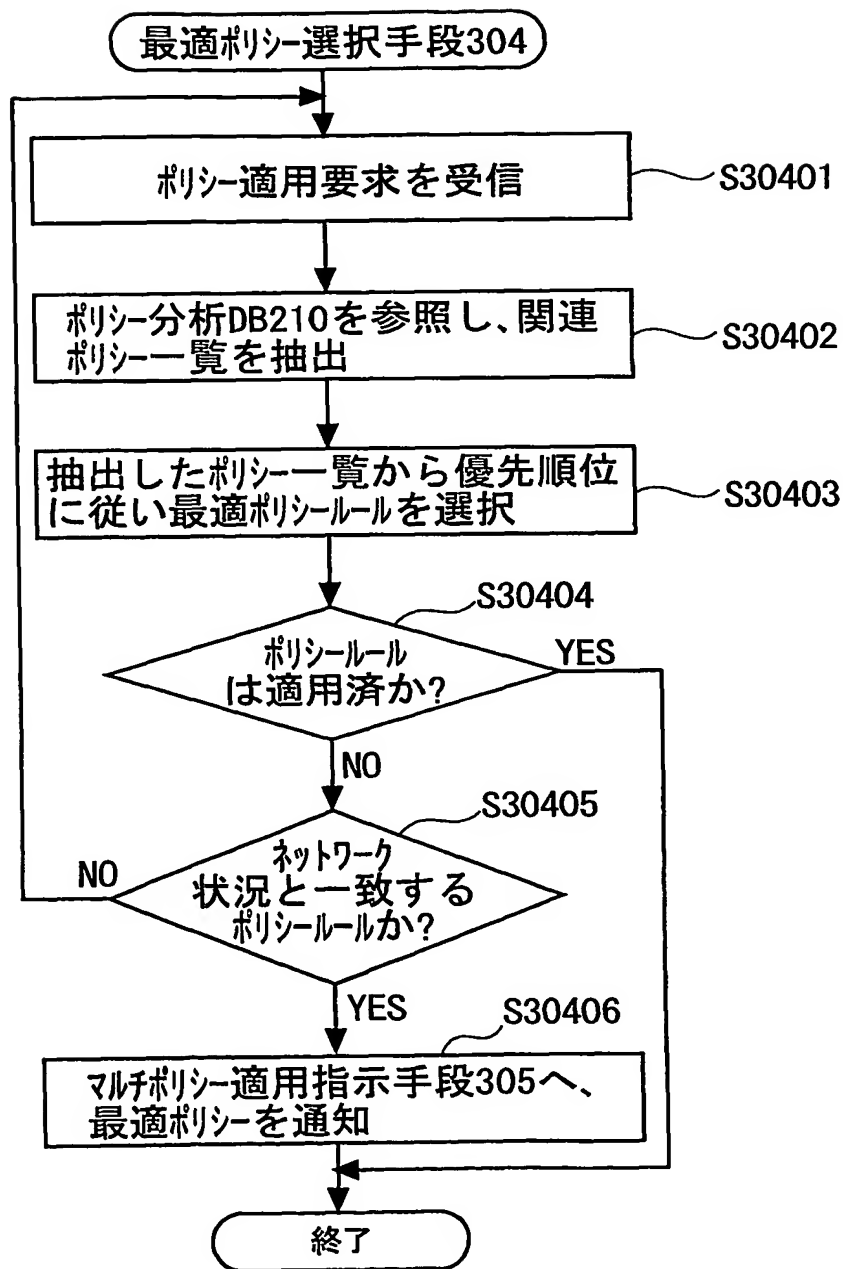
11/17

FIG. 11



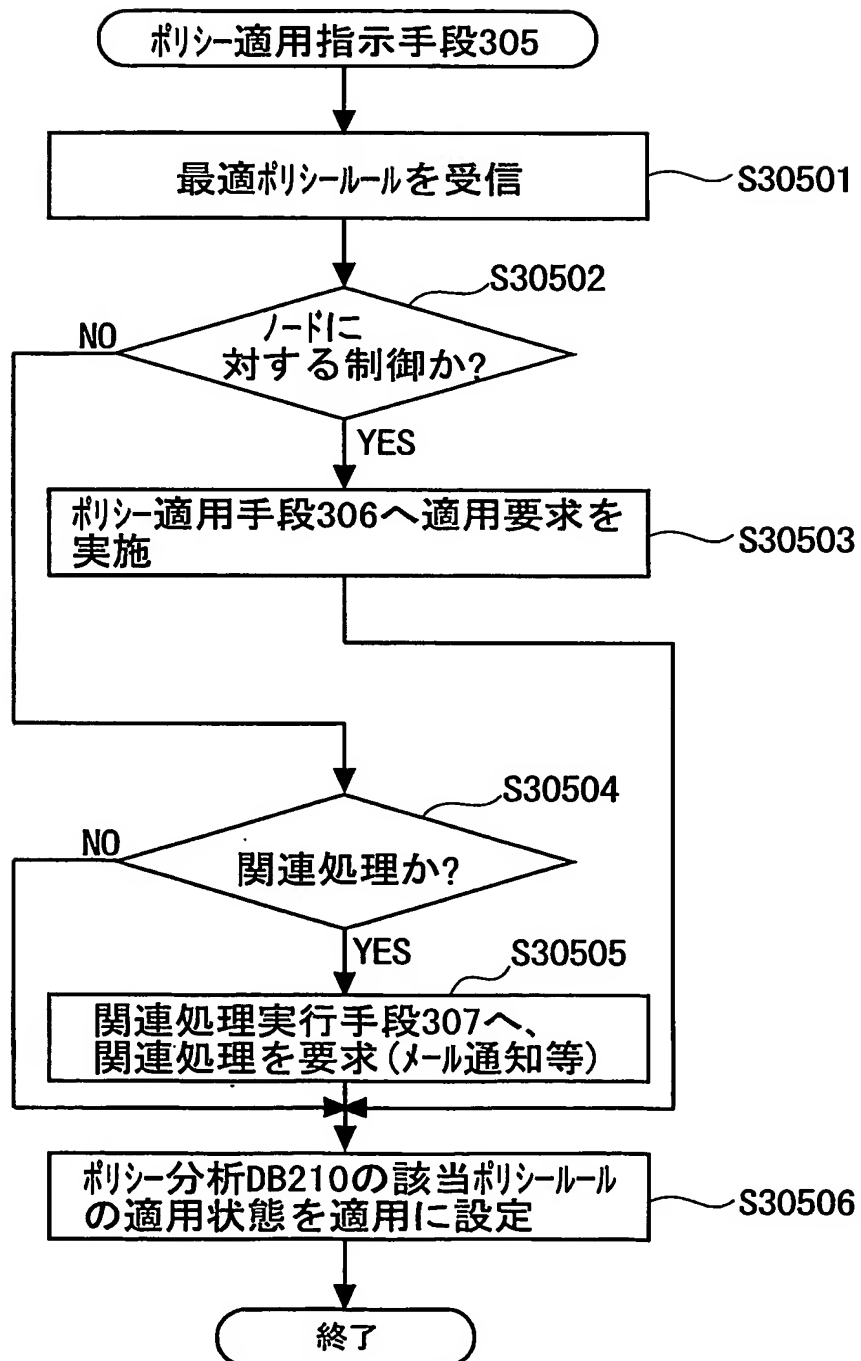
12/17

FIG. 12



13/17

FIG. 13



14/17

FIG. 14

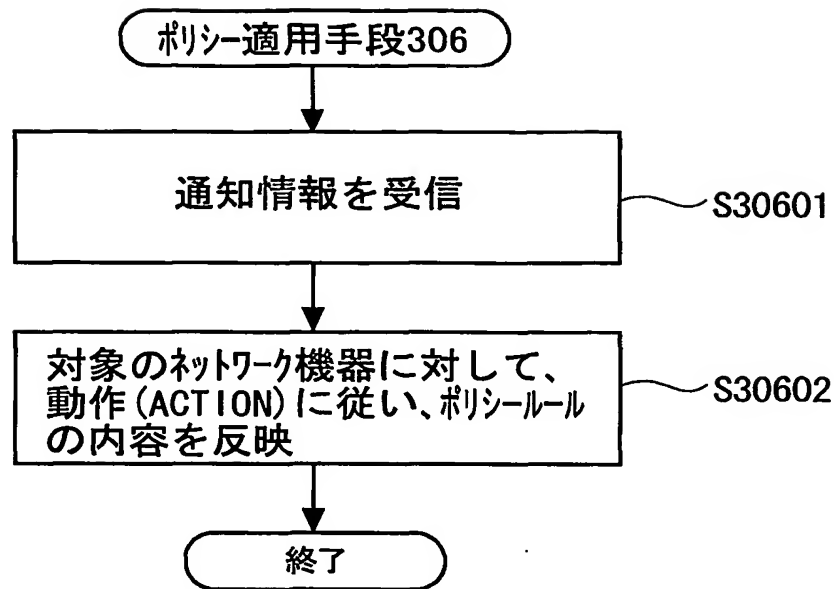


FIG. 15

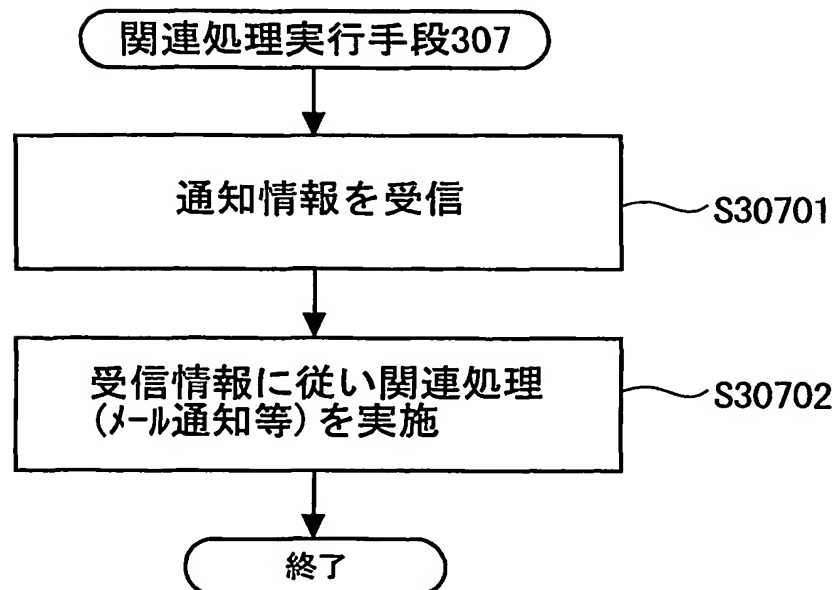
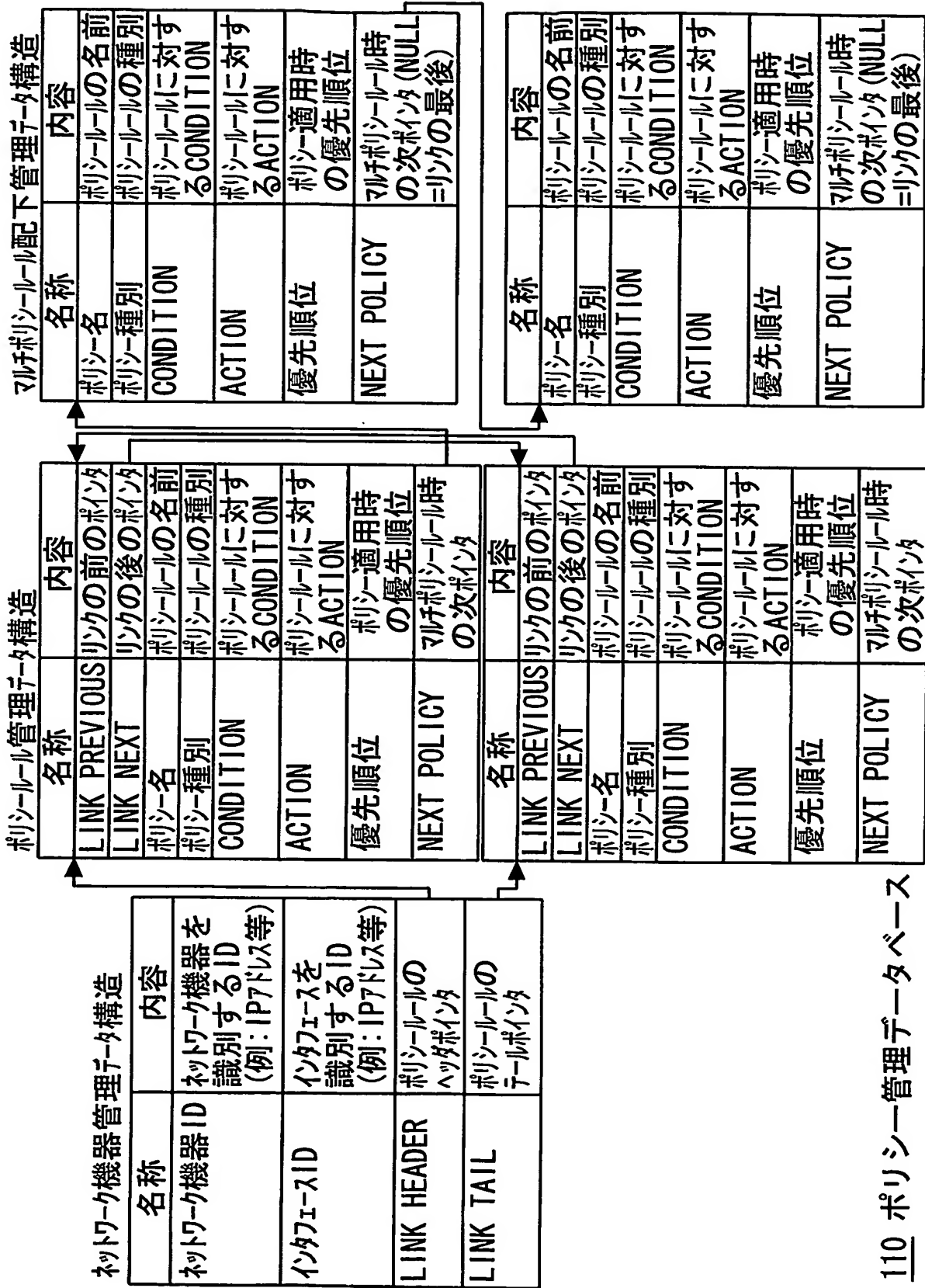
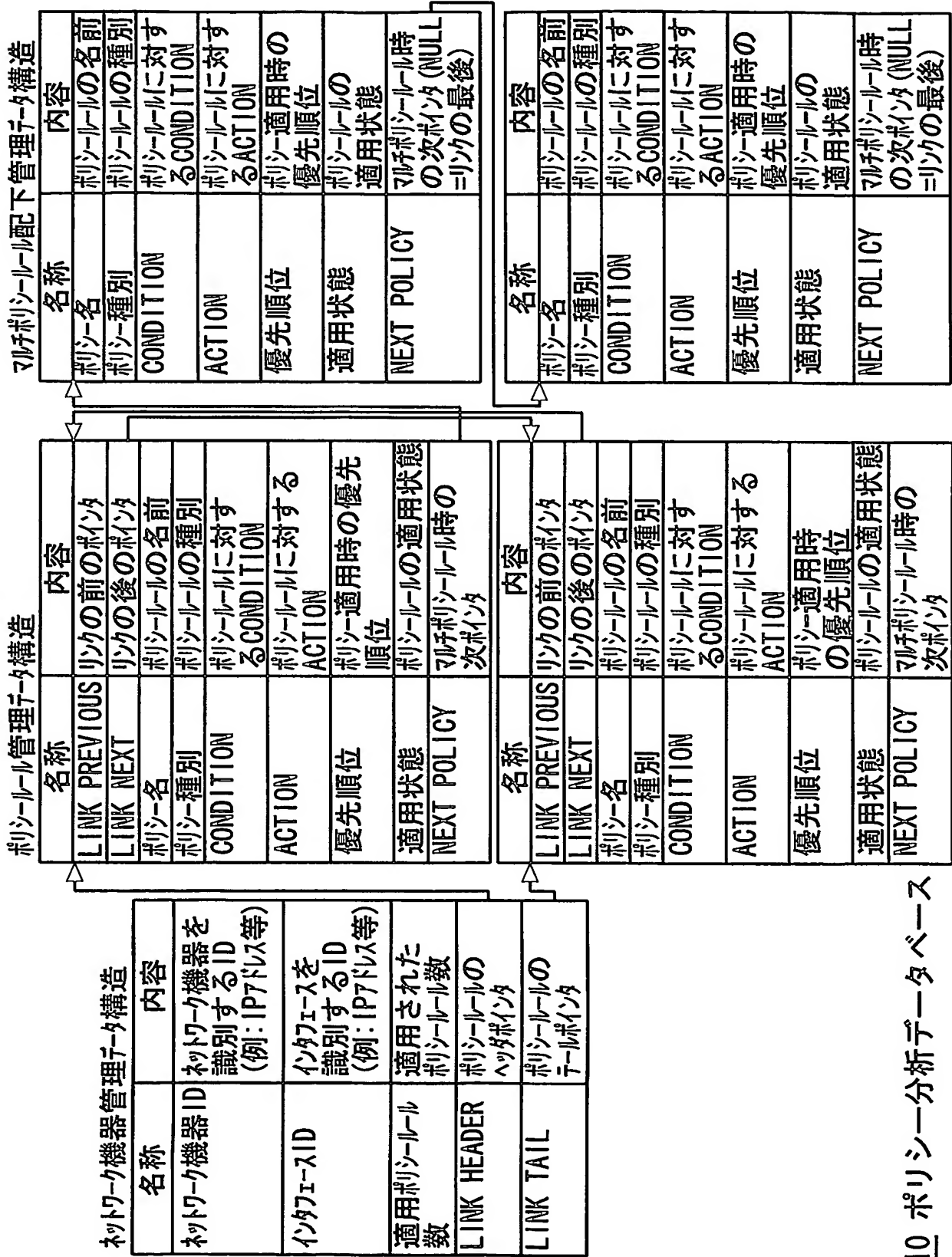


FIG. 16



16/17

FIG. 17



17/17

FIG. 18

ネットワーク機器管理データ構造

名称	内容
ネットワーク機器ID	ネットワーク機器を識別するID (例: IPアドレス等)
インタフェースID	インタフェースを識別するID (例: IPアドレス等)
ポート状態	ポートの状態 (障害等)
トラフィック量	該当インタフェースのトラフィック量
パケットロス量	該当インタフェースのパケットロス量

310 ネットワーク管理データベース

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/12726

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-173301 A (Hitachi, Ltd.), 20 June, 2003 (20.06.03), Fig. 12 (Family: none)	1-14
A	JP 2003-008624 A (Hitachi, Ltd.), 10 January, 2003 (10.01.03), Figs. 2 to 4 (Family: none)	1-14
A	JP 2002-111729 A (KDDI Corp.), 12 April, 2002 (12.04.02), Fig. 1 & US 2002/0040396 A1	1-14

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
 "A" document defining the general state of the art which is not considered to be of particular relevance
 "E" earlier document but published on or after the international filing date
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other means
 "P" document published prior to the international filing date but later than the priority date claimed
 "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 "&" document member of the same patent family

Date of the actual completion of the international search 08 January, 2004 (08.01.04)	Date of mailing of the international search report 27 January, 2004 (27.01.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

国際調査報告

国際出願番号 PCT/JP03/12726

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int. Cl⁷ H04L12/56

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))
Int. Cl⁷ H04L12/56

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年
日本国公開実用新案公報 1971-2004年
日本国登録実用新案公報 1994-2004年
日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2003-173301 A (株式会社日立製作所)、2003.06.20、図12 (ファミリー無し)	1~14
A	JP 2003-008624 A (株式会社日立製作所)、2003.01.10、図2~4 (ファミリー無し)	1~14
A	JP 2002-111729 A (ケイディーディーアイ株式会社)、2002.04.12、図1 & US 2002/0040396 A1	1~14

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日 08.01.2004

国際調査報告の発送日 27.1.2004

国際調査機関の名称及びあて先
日本国特許庁 (ISA/JP)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)
石井 研一

5 X 8124

電話番号 03-3581-1101 内線 3556